Kader Informatiebeveiliging – Authenticatie: gebruikersnamen en wachtwoorden

versie 1.0 | 19 januari 2021 | AIB-K-01.01

Leeswijzer

Dit kaderdocument is een nadere uitwerking van het 'Amsterdam UMC Informatie Beveiligingsbeleid' in vastgestelde beheersmaatregelen. In artikelen worden de maatregelen uitgewerkt die gelden voor dit domein.

De artikelen zijn voor een belangrijk deel gebaseerd op de NEN7510-2. Daarnaast gelden bij het vaststellen van de artikelen de security architectuur principes, adviezen van de leverancier over de inrichting (*best practices*) en het ontwerp en inrichting van de gehele ICT-infrastructuren van het Amsterdam UMC.
Dat betekent ook meteen dat kaders en hun artikelen niet op zichzelf staan, maar een geheel aan beveiligingsmaatregelen vormen.

Om verlies, diefstal, manipulatie, of onbevoegde toegang tot gegevens te voorkomen worden maatregelen ingezet. Maatregelen kunnen vanuit verschillende perspectieven gemotiveerd worden.

- De maatregel verkleint de kans van een aanval of misbruik
- De maatregel beperkt de schade geleden door misbruik.
- Maatregelen die ingezet worden om de schade te herstellen

Doel

Goed gebruik van de juiste gebruikersnamen en wachtwoorden begint met duidelijke regels of artikelen. Deze zijn in dit kader vastgelegd. De artikelen gaan over gebruikersnamen zowel persoonlijke als functionele, het aanmaken van wachtwoorden, de bescherming ervan en eisen t.a.v. de frequentie voor verandering.

Scope

In scope zijn alle gebruikersnamen uitgegeven door het Amsterdam UMC of aangemaakt op verzoek van het Amsterdam UMC. Uitzondering zijn gebruikersnamen voor patiënten.
Wachtwoordregels gelden echter voor alle gebruikersnamen van het Amsterdam UMC.

Doelgroep

Dit kader geldt voor alle personen, die gebruik maken van door het Amsterdam UMC beschikbaar gestelde ICT-middelen. Voor deze ICT- middelen wordt een account gebruikt. Ook ontwikkelaars die ICT-(deel)systemen voor het Amsterdam UMC bouwen dienen kennis te nemen van dit beleid en ervoor te zorgen dat hun systemen hieraan voldoen.

Verdere indeling

Artikelen

1. Gebruikersnaam
   1.01 Unieke gebruikersnaam
   1.02 Identificatie bij uitgifte persoonlijke gebruikersnaam
   1.03 Per netwerkomgeving wordt een gebruikersnaam gebruikt
   1.04 De verantwoordelijke of eigenaar van elke gebruikersnaam is eenduidig belegd
   1.05 Typen gebruikersnamen of accounts
   1.06 Gebruikersnamen met verhoogde toegangsrechten
   1.07 Vermoeden van misbruik van een account
2. Wachtwoorden en Multi-factor authenticatie (MFA)
   2.01 Standaard, default of door de leverancier ingestelde wachtwoorden
   2.02 Uniek wachtwoord voor elk account
   2.03 Foutieve inlogpogingen
   2.04 Opslaan van wachtwoorden
   2.05 Wachtwoord regels
   2.06 PIN code
   2.07 Herstellen van toegang door wachtwoord reset
   2.08 Multi-factor authenticatie (MFA)
   2.08 Step-up authenticatie
3. Bijzondere gebruikersaccounts
   3.01 Functionele accounts
   3.02 Functionele Technische accounts
   3.03 Functionele Noodaccounts
   3.04 Cursus accounts
4. Overige
   4.01 Delen van eenmalige wachtwoorden met derden
   4.02 Delen van eenmalige wachtwoorden in verband met onderhoud door leverancier
5. Uitzonderingen of excepties op dit kader
   5.01 Excepties op dit kader
   5.02 Wijzigingen op het systeem met een bestaande exceptie
6. Samenvatting gebruikersaccounts
   Accounts binnen het Amsterdam UMC

Documenthistorie

Begrippenlijst A - Z

Artikelen

1. Gebruikersnaam

1.01 Unieke gebruikersnaam

Beschrijving	Elke natuurlijke persoon wordt voorzien van een unieke gebruikersnaam of identificatiecode voor persoonlijk gebruik.	
Motivatie	Een unieke identificatiecode is nodig voor het kunnen herleiden van toegang tot gegevens aan een persoon.	
Maatregel	Identificatiecodes worden zoveel mogelijk geregistreerd in de centrale accountdirectory	• Microsoft Active Directory
	Er worden ondubbelzinnige gebruikersnamen toegepast	• Elke gebruikersnaam wordt slechts eenmaal toegepast
Noot	*Gekozen is voor de term 'gebruikersnaam' in navolging van Logius in plaats van het meer technische 'gebruikersidentificatie' uit de NEN7510, waarmee hetzelfde wordt bedoeld*	

1.02 Identificatie bij uitgifte persoonlijke gebruikersnaam

Beschrijving	Persoonlijke gebruikersnamen zijn toegewezen aan natuurlijke personen	
Motivatie	Werken met bijzondere persoonsgegevens vraagt om de juiste beveiligingsmaatregelen passend bij de risicoklasse van gegevens, zoals gesteld in NEN7510 7.1.1 (screening) en 9.2.1 (registratie en afmelden van gebruikers).	
Maatregel	Bij indiensttreding krijgt elke medewerker één gebruikersnaam die toegang geeft tot de Amsterdam UMC ICT diensten	• Persoonlijk account
	Om (buitengewone) persoonsgegevens te beschermen moet er voldaan worden aan het eIDAS betrouwbaarheidsniveau[1] 'substantieel'.	Hiervoor is authenticatie Level of Assurance (LoA)[2] niveau 3 vereist. • Fysieke check en • Tonen wettig identiteitsbewijs medewerker
Noot	[1] *eIDAS betrouwbaarheidsniveau 'substantieel'* https://www.eherkenning.nl/vraag-antwoord/betrouwbaarheidsniveaus [2]*LoA* https://wiki.surfnet.nl/display/SsID/Levels+of+Assurance,	

1.03 Per netwerkomgeving wordt een gebruikersnaam gebruikt

Beschrijving	Een gebruikersnaam per netwerkomgeving	
Motivatie	Verschillende netwerkomgevingen kunnen verschillende beveiligingsniveaus hebben en privileges. Daarom moeten hiervoor verschillende accounts worden gebruikt en als zodanig herkenbaar zijn.	
Maatregel	Productie, acceptatie en andere omgevingsaccounts verschillen van elkaar en zijn als zodanig herkenbaar.	• Onderscheid door middel van de suffix zoals acc.amc.nl • @amsterdamumc.nl uitsluitend voor het productie account • Of, door onderscheid in de gebruikersnaam

1.04 De verantwoordelijke of eigenaar van elke gebruikersnaam is eenduidig belegd

Beschrijving	Elke gebruikersnaam heeft een eigenaar, die verantwoordelijk is voor het zorgvuldig gebruik van dit account.	
Motivatie	NEN7510-9.2.1 (registratie en afmelden van gebruikers) Het gebruik van unieke gebruikersidentificaties zodat gebruikers kunnen worden gekoppeld aan en verantwoordelijk kunnen worden gesteld voor hun acties. Het gebruik van groepsidentificaties behoort alleen te worden toegelaten als deze om bedrijfs- of operationele redenen noodzakelijk zijn en behoort te worden goedgekeurd en gedocumenteerd	
Maatregel	**Gebruikersnaam**	**Eigenaar**
	Persoonlijke gebruikersnaam	• Gebruiker aan wie de gebruikersnaam is uitgereikt tijdens uitgifte
	Functioneel, technische of lokale gebruikersnaam – gebruikersgroep beperkt tot 1 afdeling	• Manager afdeling of afdelingshoofd
	Functioneel, technische of lokale gebruikersnaam – gebruikersgroep overstijgt 1 afdeling	• (overkoepelende) manager
	Functioneel, technische of lokale gebruikersnaam – gebruikersgroep beperkt tot 1 organisatie	• Directeur
	Functioneel, technische of lokale gebruikersnaam – gebruikersgroep beslaat meerdere organisatie onderdelen	• Directeur Dienst ICT

1.05 Typen gebruikersnamen of accounts

Beschrijving	Gebruikersnamen worden ingedeeld naar persoonlijke en gedeelde gebruikersnamen	
Motivatie	Primair heeft elke persoon één persoonlijk account voor dagelijkse werkzaamheden. Ook verkrijgt dit account door middel van groepslidmaatschappen, toegang tot de juiste applicaties, bedrijfs- of patiëntengegevens. Daarbovenop kan een medewerker voor het uitvoeren van specialistische taken of (eenmalige) beheerwerkzaamheden aanvullende rechten nodig hebben. Hiervoor worden dan afzonderlijke persoonlijke of gedeelde accounts ingericht. Een gedeelde gebruikersnaam heeft meer beveiligingsrisico's dan een persoonlijke gebruikersnamen.	
Maatregel	Persoonlijke standaard gebruikersnaam – Voor dagelijkse werkzaamheden en kantoorgebruik	• Persoonlijke inlog • Office toepassingen • E-mail • Autorisaties via groepslidmaatschappen a.d.h.v. functie
	Functionele gebruikersnamen - Gedeelde gebruikersnaam met groep personen	• Specifieke gezamenlijk taak • Inloggen via netwerk toegestaan
	Technische gebruikersnamen – worden alleen door en tussen systemen gebruikt	• Inloggen via netwerk **niet** toegestaan • Tussen besturingssysteem en middleware
	Lokale gebruikersnamen - worden alleen door en tussen systemen gebruikt, maar dan uitsluitend met gebruikersnamen aangemaakt op het lokale systeem	• Inloggen via netwerk **niet** toegestaan • Tussen besturingssysteem en middleware • Opstarten lokale functionaliteit

	Beheer of admin gebruikersnamen met verhoogde toegangsrechten - Beheerders	• Persoonlijke admin accounts met verhoogde privileges • Admin account wordt gebruikt naast standaard account

1.06 Gebruikersnamen met verhoogde toegangsrechten

Beschrijving	Gebruikersnamen met verhoogde toegangsrechten hebben toegang tot kritische (delen) van systemen, de IT-infrastructuur, of toegang tot vertrouwelijke informatie. Ook kunnen ze autorisaties aan anderen verstrekken of juist intrekken. Een account met verhoogde toegangsrechten kan zowel een gedeeld functionele gebruikersnaam of een persoonlijk admin gebruikersnaam zijn.	
Motivatie	Gebruikersnamen met verhoogde toegangsrechten, zijn vaak het doelwit van tegenstanders of hackers. Door ervoor te zorgen dat gebruikers met deze rechten, niet de mogelijkheid hebben om e-mails te lezen, op internet te surfen of bestanden te verkrijgen via online diensten, zoals instant messaging of sociale media, wordt de mogelijkheid dat hun accounts worden misbruikt, beperkt.	
Maatregel	Onder accounts met verhoogde toegangsrechten worden een of meerdere van de volgende items verstaan.	Deze accounts hebben de mogelijkheid: • om belangrijke systeemconfiguratie-instellingen te wijzigen • om beveiligingsmaatregelen te wijzigen of te omzeilen • tot toegang van audit- en beveiligingsmonitoring-informatie • toegang tot gegevens, bestanden en accounts die door andere gebruikers worden gebruikt, inclusief back-ups en shares en e-mail • toegang hebben om technische problemen op een systeem op te lossen • kunnen rechten en autorisatie uitdelen of intrekken
	Functionele accounts met verhoogde toegangsrechten moeten zoveel mogelijk vermeden worden door gebruik te maken van rollen en groepslidmaatschap van persoonlijke accounts.	Pas de onderstaande volgorde toe; 1. geef persoonlijke accounts de juiste groepsrechten 2. een admin-account (bij frequent gebruik door dienst ICT) 3. functioneel gedeeld account
	Gebruikers die dagelijks (of zeer frequent) met verhoogde toegangsrechten moeten werken vanuit hun functie, krijgen een separaat admin-account toegewezen. Dit account mag uitsluitend worden gebruikt voor beheertaken waarvoor deze toegang vereist is.	• Voor beheerswerkzaamheden van de Dienst ICT of door applicatiebeheerders, wordt een separaat, admin-account gebruikt • Dit account is persoonlijk

	Een account met verhoogde toegangsrechten heeft geen of zeer beperkte toegang tot kantoorapplicaties. Hierdoor wordt voorkomen dat het account voor dagelijkse kantoorwerkzaamheden wordt ingezet en wordt dus de kans op cybersecurity incidenten verkleind.	Door technische maatregelen is geborgd, dat • Er geen toegang tot e-mail • Beperkte internet toegang tot alleen vertrouwde websites • Geen toegang tot online bestanden
	Het gebruik van accounts met verhoogde rechten en alle activiteiten die daarmee worden ondernomen, worden vastgelegd in centrale logging	• Audit en loggen actief op accounts met hoge toegangsrechten
Noot	*Functionele accounts zijn door gedeeld gebruik kwetsbaarder dan persoonlijke accounts*	

1.07 Vermoeden van misbruik van een account

Beschrijving	Een gebruiker die misbruik met zijn account vermoedt dient direct het wachtwoord behorende bij dit account te veranderen en het incident te melden aan de Dienst ICT Servicedesk.	
Motivatie	Misbruik van een account kan grote impact hebben bij een organisatie als het Amsterdam UMC, het is essentieel dat bij misbruik zo snel mogelijk acties ondernomen worden om de impact te beperken	
Maatregel	Wijzigen van het wachtwoord door de medewerker	• Wijzig direct het wachtwoord
	Bij diefstal van apparatuur en bij vermoedens of sterke aanwijzingen van bijvoorbeeld de security afdeling, dat het wachtwoord gelekt is, wordt het wachtwoord gewijzigd.	• Bij een vermoedelijk gelekt wachtwoord wijzig dit direct in een nieuw wachtwoord
	Incident melden	• Meldt altijd het incident bij de Servicedesk of CERT • Ook als het wachtwoord al gewijzigd is
Noot	*Incident melding via telefoonnummer (020 566) 3011 of, buiten werktijd bij het Amsterdam UMC Computer Emergency Response Team (CERT) via (020 566) 2378*	

2. Wachtwoorden en Multi-factor authenticatie (MFA)

Noot	*Onderstaande artikelen voor wachtwoorden gelden ook voor accounts van patiënten*

2.01 Standaard, default of door de leverancier ingestelde wachtwoorden

Beschrijving	Vaak wordt er een standaard wachtwoord, in software, applicaties of hardware vanuit de leverancier ingesteld.	
Motivatie	Standaard (of default) wachtwoorden zijn makkelijk terug te vinden in de documentatie of op het internet. Hierdoor is het wachtwoord niet geheim en biedt dit geen security bescherming.	
Maatregel	Standaard ingestelde wachtwoorden	• Tijdens installatie en/of in gebruik name van een systeem of applicatie, moeten alle standaard (default) wachtwoorden veranderd worden
	Hier wordt aan de wachtwoordregels voldaan	• Zie 2.05
Noot	*Uitgezonderd zijn systemen in een testomgeving*	

2.02 Uniek wachtwoord voor elk account

Beschrijving	De gebruiker zorgt ervoor dat het wachtwoord uniek blijft, en niet hergebruikt wordt voor andere (ook niet-Amsterdam UMC) accounts	
Motivatie	Om vertrouwelijkheid van het wachtwoord te waarborgen is het essentieel dat het alleen bij de gebruiker bekend is. Bovendien moet de gebruiker een wachtwoord kiezen dat goed te onthouden is zonder dat hij het op hoeft te schrijven.	
Maatregel	De gebruiker zorgt ervoor dat het wachtwoord uniek blijft, en niet hergebruikt wordt voor andere (ook niet-Amsterdam UMC) accounts	• Wachtwoord blijft uniek • Voor elk account binnen het Amsterdam UMC, wordt een ander wachtwoord gekozen • Voor elk account buiten het Amsterdam UMC, wordt een ander wachtwoord gekozen

2.03 Foutieve inlogpogingen

Beschrijving	Foutief opgeven van de gebruikersnaam, het bijbehorende wachtwoord of token.	
Motivatie	Door het blokkeren van een account na een bepaald aantal mislukte aanmeldingspogingen, wordt de kans op succesvolle aanvallen met gerade wachtwoorden verkleind. Er moet echter op worden gelet dat het implementeren van account blokkade, de kans op een denial of service (DoS) kan vergroten.	
Maatregel	Account blokkeren na een aantal mislukte inlogpogingen. Indien technisch mogelijk, moet er pauze worden ingesteld vanaf de derde loginpoging bv. 3de poging: pauze tot de volgende login 5 minuten 4de poging: pauze tot de volgende login 10 minuten	• Na 5 mislukte pogingen • Indien technisch mogelijk vanaf de derde poging tussenpozen tussen elke volgende poging
	Duur blokkade	• 30 minuten, of • Tot een beheerder het account vrij geeft

	Herhaling van account blokkades worden onderzocht	• Foutieve en succesvolle inlogpogingen worden gelogd • Herhaalde blokkade genereert een alert waarop actie wordt ondernomen

2.04 Opslaan van wachtwoorden

Beschrijving	De gebruiker slaat het wachtwoord niet leesbaar op, in welke vorm dan ook zodat deze geheim blijft. Ze mogen dus niet worden opgeschreven, uitgeprint, opgeslagen op harde schijf, USB stick, enzovoort	
Motivatie	Cryptografische methoden die worden gebruikt om wachtwoorden wel veilig op te slaan dienen vooraf te worden getoetst en goedgekeurd door Dienst ICT Security. Als cryptografie (versleuteling) gebruikt wordt, moet dit ook gegarandeerd het doel ondersteunen dat alleen bevoegde personen toegang hebben tot de informatie. Omdat cryptografie een complex kennisgebied is en ook sterk afhankelijk van de juiste configuratie, kan alleen door een specialist bepaald worden of de gebruikte technieken voldoende veiligheid bieden.	
Maatregel	Leesbaar opslaan op shares, USBs, maar ook in scripts of batches	• Niet toegestaan
	Gebruik van cryptografie	• Alleen geaccordeerde encryptiemethoden zijn toegelaten (zie cryptografie) • Altijd in combinatie met een wachtwoord volgens 2.05
	Wachtwoordkluizen	• Alleen de gecentraliseerde kluis is toegestaan geaccordeerd door Dienst ICT Security
	Het wachtwoord mag niet in de browser opgeslagen worden via opties als “*remember my password*”, ”onthoudt mijn wachtwoord”, enzovoort	• Niet opslaan in browser cache

2.05 Wachtwoord regels

Beschrijving	Regels waaraan een wachtwoord of een wachtzin moet voldoen	
Motivatie	Wachtwoorden zijn voldoende complex om “kraken”, raden of afkijken tegen te gaan. Het nieuwe wachtwoord mag niet lijken op het oude wachtwoord, of gelijk zijn aan één van de eerdere gebruikte wachtwoorden, zodat zelfs ‘gekraakte’ wachtwoorden hun geldigheid verliezen. Het gebruik van een ‘wachtzin’ wordt aangemoedigd doordat deze beter te onthouden zijn, unieker zijn (er wordt niet met volgnummers gewerkt) en door de lengte zeer moeilijk te kraken zijn	
Maatregel	Geldigheidsduur initieel wachtwoord bij eerste login	• 24 uur
	Geldigheidsduur na wachtwoord reset door beheerder	• 24 uur
	Het nieuwe wachtwoord mag niet lijken op het oude wachtwoord, of gelijk zijn aan één van de laatst gebruikte wachtwoorden	• 24 unieke wachtwoorden
	Minimale wachtwoordlengte: Standaard Persoonlijke admin-accounts Overige admin-accounts	 • 8 karakters • 14 karakters • 16 karakters
	Wachtwoord samenstelling	• Hoofdletters • Kleine letters • Cijfers • 1 speciaal teken

	Een wachtwoord mag niet bestaan uit (delen van) de gebruikersnaam	• Wachtwoord lijkt niet op de gebruikersnaam
	Wachtwoord vernieuwen	• Elke 9 maanden, of • bij een (vermoeden van) gecompromitteerd wachtwoord
Noot	*Voorbeelden van speciale tekens, naast het 'spatie-teken' en 'punt', zijn* ()!@#$%&,.	

2.06 PIN code

Beschrijving	Voorwaarden waaraan pincodes moeten voldoen	
Motivatie	Een pincode moet voldoende veilig zijn en bestand zijn tegen raden. Hiervoor is een minimale lengte nodig en moeten reeksen vermeden worden.	
Maatregel	PIN Code voor intern gebruik	• Minimaal 4 karakters • Eenvoudige nummerreeksen, zoals 1234 of 0000, zijn niet toegestaan • Reeksen van herhaalde nummers zoals 2233 of 3344, zijn niet toegestaan
	Mag alleen toegepast worden in combinatie met multi-factor authenticatie (MFA)	• In combinatie met MFA • Zie 2.08
	Andere eisen	• Zie 2.05
Noot		

2.07 Herstellen van toegang door wachtwoord reset

Beschrijving	Herstellen van de toegang door het wachtwoord of wachtzin te vervangen door een nieuwe.	
Motivatie	Om de kans te verkleinen dat *social engineering* wordt gebruikt om accounts te compromitteren, moeten gebruikers voldoende bewijs leveren om hun identiteit te verifiëren bij het aanvragen van een account herstel.	
Maatregel	Gebruikers leveren voldoende bewijs om hun identiteit te verifiëren bij het aanvragen van een wachtwoord reset van hun persoonlijke standaard account	• Fysiek verschijnen met een geldig identiteitsbewijs[2]
	Het opnieuw instellen van een wachtwoord is willekeurig	• Servicedesk stelt uniek wachtwoord in voor elk verzoek • en is niet gebaseerd op een andere identificerende factor zoals de naam van de gebruiker of de geboortedatum.
	Nadat het wachtwoord voor de eerste maal door de Dienst ICT is uitgereikt dient het door de gebruiker veranderd te worden.	• Gebruiker wijzigt direct het wachtwoord (volgens 2.05) • Uiterlijk binnen 24 uur
Noot	*[2]Bij persoonlijk standaard account moet voldoen aan LoA 3*	

2.08 Multi-factor authenticatie (MFA)

Beschrijving	Voordat toegang tot een systeem en zijn bronnen aan een gebruiker wordt verleend, is het essentieel dat ze worden geauthentiseerd. Dit wordt doorgaans bereikt via meervoudige authenticatie, zoals een gebruikersnaam samen met biometrische gegevens en een wachtwoord.	
Motivatie	Door het gebruik van een aanvullende inlogmethode, bijvoorbeeld naast het wachtwoord, neemt de zekerheid dat de persoon die een gebruikersnaam toepast, ook de daadwerkelijke natuurlijke persoon is. Hierbij wordt er op gelet dat er van minstens twee verschillende factoren gebruik wordt gemaakt en niet tweemaal dezelfde factor gebruik wordt gemaakt. (NEN7510-9.4.1, Beperking toegang tot informatie)	
Maatregel	Kennis bezit of lichaamskenmerk	• 2-factor authenticatie (2FA) • Kennisfactor • Bezitsfactor
	Multi-factor authenticatie gebruikt minstens 2 van de volgende authenticatie factoren	• Wachtwoord • Universal 2nd Factor security keys (U2F open standaard) zoals Yubikey • Fysieke one-time password (OTP) tokens • Biometrische gegevens of • Smartcards
	Kennisfactor is een geheime en persoonlijke code in de vorm van een wachtwoord of pin code	• Wachtwoord • PIN code
	Wachtwoord voldoet aan de Amsterdam UMC wachtwoordregels	• Zie 2.05

	Standaard oplossing voor de bezitsfactor, gebruikt door Amsterdam UMC, is	• SURFsecureID waarbij;
		  ○ TIQR authenticatie app geïnstalleerd op smartphone in bezit van de werknemer of,
		  ○ Yubikey in bezit van de werknemer

	Multi-factor authenticatie wordt gebruikt voor de volgende accounts	• Gebruikers met remote toegang • Gebruikersnamen die toegang geven over onveilige netwerken of het internet

2.08 Step-up authenticatie

Beschrijving	Met step-up authenticatie hebben medewerkers toegang tot de gegevens die ze elke dag nodig hebben, zonder automatisch toegang te krijgen tot gevoelige bronnen. Zodra ze toegang tot gevoelige bronnen nodig hebben, kan step-up authenticatie ze opnieuw verifiëren met een ander wachtwoord.	
Motivatie	Meerdere niveaus van toegang is een belangrijk beschermingsprincipe (“defence in depth”), waarbij als een laag wordt gecompromitteerd de volgende laag alsnog de aanval stopt of aanzienlijk de impact van de schade beperkt. Door hetzelfde wachtwoord voor verschillende niveaus te gebruiken, wordt het beschermingsprincipe teniet gedaan.	
Maatregel	Als een één-factor systeem de mogelijkheid biedt van meerdere niveaus van toegang op basis van één inlog UID en een “step-up” authenticatie (bijvoorbeeld “alleen lezen” versus “lezen plus wijzigen”) dan dienen hiervoor verschillende wachtwoorden gebruikt te worden.	• Gebruik voor Step-up verschillende wachtwoorden

3. Bijzondere gebruikersaccounts

3.01 Functionele accounts

Beschrijving	Functionele accounts zijn gedeelde accounts voor een specifiek omschreven taak of taken. Het delen van een functioneel account met een groep gebruikers, gebeurt vaak doordat het wachtwoord bij deze groep toegankelijk is.	
Motivatie	Functioneel accounts hebben vaak specialistische bevoegdheden om taken van een afdeling uit te voeren. Bij sommige van deze accounts is er ook sprake van hoge toegangsrechten (denk aan de IT-beheerders voor het resetten van wachtwoorden). Doordat functionele accounts gebruikt kunnen worden door verschillende gebruikers, zijn aanvullende maatregelen nodig om de herleidbaarheid tot individuen mogelijk te maken. Daarnaast is er een risico dat er autorisaties worden uitgedeeld via een functioneel account zonder dat dit transparant is, zoals dat met de uitgifte van groepslidmaatschappen op basis van *Role based access* (RBAC).	
Maatregel	Elk functioneel account heeft een eigenaar, die verantwoordelijk is voor het zorgvuldig gebruik van zijn account.	Dit houdt in dat hij bewaakt dat • het account voldoet aan alle artikelen gesteld in dit kader
	Functionele accounts mogen gebruikt worden wanneer taken gedeeld worden door een groep (specialistische) gebruikers en het door de aard van werkzaamheden aannemelijk is dat individuele accounts het werk onnodig complex maken en hierdoor een verhoogd security risico vormen – of wanneer zorgprocessen hierdoor gevaar lopen.	• de eigenaar motiveert de zakelijke noodzaak om gebruik te maken van een functioneel in plaats van een persoonlijk account. • Deze motivatie moet regelmatig opnieuw worden getoetst
	De rechten van gedeeld account zijn zo beperkt mogelijk	• alleen de privileges of rechten die uitsluitend noodzakelijk zijn om de werkzaamheden goed te kunnen uitvoeren (principe *need-to-use*)
	Gebruikers van een functioneel account is beperkt tot een selecte groep medewerkers	• Alleen medewerkers met een noodzaak om hun werk te kunnen uitvoeren, hebben toegang tot een functioneel account (principe *need-to-know*)
	Het gebruiken van een functioneel account moet altijd herleidbaar zijn tot een individuele persoon.	• Minimaal geldt dat er aan de hand van logfiles te herleiden is wie een functioneel account gebruikt heeft.
	Het gebruiken van een functioneel account met *verhoogde toegangsrechten*, wordt strikt gecontroleerd en moet altijd herleidbaar zijn tot een individuele persoon.	Functioneel account met verhoogde toegangsrechten: • Er is een proces actief waarbij de gebruiker eerst geïdentificeerd wordt aan de hand van zijn standaard account, voorafgaand aan het ophalen van het wachtwoord[1]
	Functionele accounts moeten worden getoetst of de individuele gebruikers nog een zakelijke noodzaak hebben om dit account te mogen gebruiken	• Verander het wachtwoord na een wijziging van de samenstelling gebruikers • Indien er geen noodzaak meer bestaat, wordt de gebruiker uitgesloten (door bv. Een

		wachtwoord wijziging van het functionele account)
Noot	*Zie ook 1.06 Accounts met verhoogde toegangsrechten*	

3.02 Functionele Technische accounts

Beschrijving	Voor het uitvoeren van beheerswerkzaamheden op ICT-middelen zijn zogenaamde “technische accounts” (root, administrator, power user, super user, enzovoort.) noodzakelijk.	
Motivatie	Functionele technische accounts behoren tot accounts met de hoogste privileges en zijn vaak doelwit van cybercriminelen.	
Maatregel	Het gebruik van (gedeelde) functionele admin accounts moet ontmoedigt worden	• Voor dagelijkse werkzaamheden zijn de rechten belegd bij het persoonlijke admin-account van de medewerker
	Systeemprocessen draaien onder een eigen gebruikersnaam (een functioneel account), voor zover deze processen handelingen verrichten voor andere systemen of gebruikers	• Systeemprocessen hebben een eigen gebruikersnaam
	Er mag niet direct met functionele admin-accounts ingelogd worden. Een beheerder logt dus in met zijn persoonlijke account en wachtwoord. Na succesvol inloggen kan hij doorloggen naar het admin-account door gebruik te maken van de admin-gebruikersnaam en -wachtwoord	• Eerst authentiseren met persoonlijk account • Vervolgens met admin-account

3.03 Functionele Noodaccounts

Beschrijving	Noodaccounts zijn een type admin-accounts en hebben (uitzonderlijk) hoge toegangsrechten op systemen, applicaties, netwerken en Cloud diensten. Daarnaast moeten deze accounts eenvoudig beschikbaar zijn bij calamiteiten.	
Motivatie	Noodaccounts met hoge privileges, moeten met name tijdens grote incidenten beschikbaar zijn met zo min mogelijk technische beperkingen. Ook kunnen ze ingezet worden voor zeldzame ‘high level’ aanpassingen. Daarentegen vragen deze accounts aanvullende bescherming gezien de hoge privileges die deze accounts doorgaans hebben.	
Maatregel	Gebruik van Noodaccounts	• in geval van grote, disruptieve incidenten • Incidentele modificatie waarbij uitzonderlijke aanpassingen nodig zijn op het systeem die alleen met deze rechten kunnen worden doorgevoerd
	Wachtwoord wijziging	• Alleen na gebruik
	Om de beschikbaarheid te vergoten kunnen noodaccounts, met aanvullende maatregelen uitgezonderd worden van verschillende wachtwoordregels en multi-factor authenticatie.	• Afhankelijk van beschikbaarheidscriteria, geen MFA • Wachtwoord 16 karakters • Bij voorkeur gebruik van 4-ogen principe

	Strikt *Least privilege* principe	• Beheeraccounts mogen niet, door bijvoorbeeld groepslidmaatschap, dezelfde privileges verwerven als nood accounts
	Strikt *Need-to-know* principe	• Alleen een zo klein mogelijke groep geautoriseerde personen kent het bijbehorende wachtwoord
	Om beschikbaarheid te garanderen wordt van elk noodaccount een extra account gemaakt met dezelfde privileges.	• Er zijn 2 tot 3 Noodaccounts met dezelfde privileges • Wachtwoorden zijn (uiteraard) verschillend
Noot	*Bij voorkeur gebruik van 4-ogen principe, logging is actief en er wordt een logalert getriggerd op gebruik van dit account*	

3.04 Cursus accounts

Beschrijving	Voor Amsterdam UMC ingestelde wachtwoorden van cursus accounts (bv. cursist1 of student10) geldt dat die gebruikt worden voor educatieve doeleinden (bv. cursus, of e-learning) in een apart netwerk	
Motivatie	Voor Amsterdam UMC wachtwoorden van cursus accounts (bv. cursist1 of student10) geldt dat zij direct geblokkeerd moeten worden wanneer de werkzaamheden (bv. cursus, of e-learning) zijn voltooid waarvoor het account bedoeld is. Ook dit soort “eenvoudige” accounts met beperkte rechten kan door een hacker gebruikt worden als een springplank naar andere gevoelige informatie.	
Maatregel	Gebruik van cursus accounts	• Accounts zijn alleen actief tijdens de cursus • Na afloop worden zij verwijderd, of • Het account wordt geblokkeerd zodat inloggen niet mogelijk is
	Wachtwoord wijziging	• Per cursus is een uniek wachtwoord ingesteld
	Verantwoordelijke eigenaar	• manager

4. Overige

4.01 Delen van eenmalige wachtwoorden met derden

Beschrijving	Een medewerker mag uitsluitend eenmalige wachtwoorden (*one time passwords* of OTP) leesbaar versturen via email, SMS, WhatsApp, fax, post, Microsoft Teams enzovoort.	
Motivatie	Eenmalige wachtwoorden hebben minder risico's op misbruik. Een eenmalig wachtwoord kan maar één keer gebruikt worden (bij voorkeur zelfs alleen binnen een beperkte tijd) en is daarna ongeldig/onbruikbaar.	
Maatregel	Delen van gebruikersnaam en systeemnaam en het wachtwoord apart	• Alle items worden gedeeld via gescheiden kanalen
	De medewerker heeft voldoende zekerheid dat alléén de beoogde ontvanger het OTP wachtwoord ontvangt	• Het gebruikte medium (telefoon of email) is al bekend

4.02 Delen van eenmalige wachtwoorden in verband met onderhoud door leverancier

Beschrijving	Als vanwege onderhoud of ondersteuning door derde of een leverancier, kennis nodig heeft van het (admin) wachtwoord, dan geldt dat na beëindiging van de betreffende onderhoudswerkzaamheden direct het account geblokkeerd of het wachtwoord gewijzigd dient te worden	
Motivatie	Deze voorwaarde is om te borgen dat de informatiebeveiliging van de desbetreffende systemen gegarandeerd blijft.	
Maatregel	Na gebruik account blokkeren of wijzigen	• Account blokkeren of, • Wachtwoord wordt gewijzigd na werkzaamheden • Niet later dan 8 uur na uitgifte • Automatiseren heeft de voorkeur
	Delen van het wachtwoord is alleen toegestaan wanneer er een overeenkomst is met de externe partij of leverancier	• Er is een verwerkers-overeenkomst vastgelegd

5. Uitzonderingen of excepties op dit kader

5.01 Excepties op dit kader

Beschrijving	Geeft aan hoe een uitzondering of exceptie op dit kader aangevraagd moet worden en aan welke voorwaarden er voldaan moet worden.	
Motivatie	Uitzonderingen worden gemanaged volgens de NEN 7510 'Pas toe – Leg uit' principe waarbij het risico's van de voorgestelde alternatieve maatregelen worden getoetst of het restrisico acceptabel is.	
Maatregel	Uitzonderingen op dit beleid zijn alleen mogelijk wanneer is voldaan aan de onderstaande voorwaarden:	
	Vastgesteld is door de Dienst ICT beheer dat er geen alternatieven mogelijk zijn om de gewenste functionaliteit te bieden op een manier die binnen het DMZ beleid valt en	• Vaststelling Dienst ICT beheer
	Er is een Risico Analyse (RA) uitgevoerd op de uitzonderingssituatie.	• RA opgesteld
	De Directeur Dienst ICT van mening is dat de dienst of functionaliteit van dusdanig belang voor het Amsterdam UMC is dat dit in aanmerking kan komen voor een uitzondering omdat het bedrijfsbelang opweegt tegen het extra beveiligingsrisico (gespecificeerd in de RA) dat hierdoor ontstaat.	• Uitzondering bekrachtigt door Directeur Dienst ICT
	Uitzonderingen op dit beleid wordt schriftelijk aangevraagd bij en beoordeeld door de IT Security Officer via ITSM applicatie.	• Via ServiceNow • Expliciete toestemming IT Security Officer
	Dit schriftelijk verzoek motiveert het volgende:	• Reden van de uitzondering en waarom er niet aan de eis(en) van dit kader voldaan kan worden • Inschatting van het overblijvende restrisico door de technisch specialist • Toelichting van alternatieve maatregelen
Noot	*Volgens AMC DMZ Beleid, art. 36*	

5.02 Wijzigingen op het systeem met een bestaande exceptie

Beschrijving	Wijzigingen (changes) op het systeem of op de infrastructuur, kunnen invloed hebben op de beperkte (exceptie) beveiliging.	
Motivatie	Systemen met excepties zijn kwetsbaarder voor aanvallen door cybercriminelen. Omdat het restrisico op de beveiliging van eerder afgegeven excepties door systeemwijzigingen kunnen veranderen, moet het beveiligingsrisico heroverwogen worden of dit nog steeds binnen een aanvaardbaar niveau is.	
Maatregel	Als er veranderingen plaats vinden aan de opzet van het systeem in kwestie nadat de exceptie is toegestaan conform bovenstaande procedure, dan zal door de ITSO bepaald worden of de Risico Analyse (RA) opnieuw uitgevoerd moeten worden	• Bij wijzigingen wordt er naar gestreefd de exceptie weg te nemen en zo het beveiligingsrisico te minimaliseren • Eigenaar informeert de IT Security Officer over de (aanstaande) wijziging • IT Security Officer beoordeelt of de Risico Analyse (RA)

		opnieuw moet worden uitgevoerd
	Er wordt opnieuw een Risico Analyse (RA) uitgevoerd op de uitzonderingssituatie.	• Zie 5.01
Noot	*Volgens AMC DMZ Beleid, art. 37*	

6. Samenvatting gebruikersaccounts

Accounts binnen het Amsterdam UMC

	Persoonlijk		Gedeeld			
Accounts	Persoonlijke inlog accounts	Beheer accounts	Functionele accounts	Technische accounts	Nood accounts	Cursus accounts
Naamconventie						
Voorbeeld	ppjansen	admin-ppjansen		srv_database	root	Cursus01
Eigenaar	gebruiker	gebruiker	manager	manager	manager	manager
Persoonlijk	Ja	Ja	-	-	-	-
Gedeeld account	Nee	Nee	Ja	Ja	Ja	
Privileges						
Hoge Toegangsrechten	-	Ja	mogelijk	Ja	Ja	Nee
Office en email toepassingen	Ja	Nee	Beperkt[1]	Nee	Nee	Nee
Remote login toegestaan	Ja	Ja	Ja	Nee	Ja	Ja
Multi-factor authenticatie	2FA	2FA	-	-	Soms[2]	-
Wachtwoord specificaties						
Minimale lengte	8	14	8	16	16	8
Karakters special en alfanum.	Ja	Ja	Ja	Ja	Ja	Ja
Historie unieke wachtwoorden	24	24	24	24	24	24
Wijzigen elke x maand	9	9	9	9	Na gebruik	Na elke cursus
Minimale duur in dagen	1	1	1	1	1	-
Single Sign On (SSO) toegestaan	Ja	-	-	-	-	-
Centrale kluis - verplichte opslag	-	-	Ja	Ja	Ja	-
Blokkeer ongebruikt account langer dan x dagen	90	90	30	Nooit	Nooit	Nooit
Vier-ogen principe bij gebruik	-	-	-	-	Ja	-

[1] Onder voorbehoud en alleen op exceptiebasis
[2] Noodaccounts moeten ook toegankelijk zijn als MFA niet werkt. Om het restrisico te mitigeren wat hierdoor ontstaat, wordt vier-ogen principe gevraagd en is een elektronische kluis verplicht

Documenthistorie

NEN7510-2 referenties

#	Paragraaf
9	Toegangsbeveiliging
9.1	Bedrijfseisen voor toegangsbeveiliging
9.2	Beheer van toegangsrechten van gebruikers
9.3	Verantwoordelijkheden van gebruikers
9.4	Toegangsbeveiliging van systeem en toepassing

Overige Referenties

Auteur	Titel	Bron
E. Beekman	AMC DMZ-beleid	

Versiebeheer

Datum	Versie	Auteurs	Wijzigingen
03-06-2020	v0.3	P. Leeraert	Initiële opzet a.d.h.v. NEN7510 AMC Wachtwoordbeleid v1.0
19-01-2021	v1.0	P. Leeraert	Enige correcties en goedkeuring MT Dienst IT

Distributie

Datum	Versie	Aan	Functie of rol
03-12-2020	v0.3	ASB	ASB - overleg
19-01-2021	v0.9	MT Dienst ICT	

Wijzigingen

Artikel Nummer	Titel	Wijziging
1.01		

Begrippenlijst A - Z

Zie link.