Document ID (autonummer): 004093, Titel: Wachtwoord- en authenticatiebeleid, te gebruiken tot 24 uur na, Huidige datum: 26-02-2026, Huidige tijd: 09:59 Versie: 6

NORM	ISO27002 | Praktijkrichtlijn met beheersmaatregelen op het gebied van informatiebeveiliging
HOOFDSTUK	A.9 | Toegangsbeveiliging
NORMELEMENT	A.9.2.4 | Beheer van geheime authenticatie informatie van gebruikers
BEVEILIGINGSNIVEAU	BASELINE

1. INLEIDING

MUMC+ wil de toegang tot IT-voorzieningen en gegevens beheersen met het oog op de beschikbaarheid, integriteit en vertrouwelijkheid van gegevens. Gebruikers krijgen toegang tot voorzieningen en gegevens middels een account. Hiervoor wordt gebruik gemaakt van gebruikersnamen (identificatie) en authenticatiemiddelen zoals bijv. wachtwoorden en pincodes. Authenticatiemiddelen zijn een belangrijk middel om de persoonlijk geoorloofde toegang tot de MUMC+ informatiesystemen te verschaffen en te borgen. Regels m.b.t. deze middelen worden deels door systemen afgedwongen, maar doen ook een beroep op de verantwoordelijkheid en zorgvuldigheid van gebruikers. In deze richtlijn wordt aangegeven welk beleid het MUMC+ hanteert voor het gebruik en beheer van authenticatiemiddelen. De regels gaan over het gebruik en beheer van wachtwoorden en authenticatiemiddelen, de bescherming ervan en de eisen die eraan gesteld worden.

2. DOELSTELLING

Doelstelling is om toegang op een eenduidige, veilige en tevens praktisch werkbare wijze te organiseren waarbij wet- en regelgeving en maatschappelijke eisen zijn geborgd. Op grond van de Wet op de Geneeskundige Behandelingsovereenkomst is bepaald dat alleen bevoegde gebruikers toegang mogen hebben tot (zorg) gegevens. Een eis van NEN7510/ISO27001 is dat handelingen in het informatiesysteem tot een natuurlijk persoon herleidbaar zijn. Dit stelt voorwaarden aan de gebruikersidentificatie in informatiesystemen.

3. DEFINITIES

- *MUMC-account*: unieke combinatie van gebruikersnaam en wachtwoord voor persoonlijk gebruik door medewerker MUMC+
- *persoonsgebonden account*: account dat tot een natuurlijk persoon herleidbaar is; hierbij wordt onderscheid gemaakt tussen gebruikersaccounts en beheeraccounts (accounts met extra rechten)
- *generiek account*: account dat niet herleidbaar is tot een natuurlijk persoon; hierbij kan ook onderscheid gemaakt worden tussen gebruikersaccounts en beheeraccounts (accounts met extra rechten)
- *systeem account*: account dat zonder tussenkomst van mensen functioneert. Voorbeelden waarbij deze accounts gebruikt worden: als er automatisch door een service moet worden aangemeld, apparaten met een IT-component die volstrekt autonoom functioneren en slechts één niet-direct gebruikergebonden taak uitvoeren, mogen voorzien zijn van een systeemaccount
- *identificatie*: het proces waarbij de identiteit van een persoon of een organisatie vastgesteld wordt

- *authenticatie*: het proces waarbij een identiteit (persoon/systeem) bevestigd kan worden of waarmee integriteit en herkomst van aangeboden gegevens gecontroleerd kunnen worden

4. TOEPASSINGSGEBIED

Dit beleid is van toepassing op alle binnen het MUMC+ gebruikte IT-voorzieningen. De richtlijn geldt voor alle systemen en eenieder die, al dan niet op basis van een arbeidsovereenkomst, werkzaam is voor het MUMC+ en op enigerlei wijze gebruik maakt van MUMC+ informatiesystemen. Gebruik van IT-voorzieningen impliceert dat de gebruiker zich overeenkomstig de inhoud en de strekking van het beleid zal gedragen. Voor MUMC+ is de implementatie van het wachtwoordbeleid onderdeel van de Baseline beheersmaatregelen. Uitzonderingen op het wachtwoord- en authenticatiebeleid worden vastgelegd in het Risicomemorandum.

5. BELEIDSUITGANGSPUNTEN

In het MUMC+ geldt dat er in principe onderscheid is in toegang tot data die hoog vertrouwelijk is en authenticatie op niveau Hoog (Stork QAA4) vereist, en minder vertrouwelijke data die met een lager authenticatieniveau zou kunnen worden benaderd. In de praktijk is het faciliteren van dit onderscheid echter veeleisend. Om deze reden wordt alle informatie binnen het domein van het MUMC+ benaderd op basis van Stork QAA4 authenticatie.

Het wachtwoordbeleid van MUMC+ omvat de onderstaande elementen

	ELEMENT	RICHTLIJN
1	Gebruikersnaam	Persoonlijke accounts voor gebruikers: ‘G’ + personeels-ID Persoonlijke accounts voor beheerders: ‘B’ + personeels-ID Persoonlijke accounts voor externe beheerders: ‘E’ + volgnummer Overige accounts volgen de normeringen van MIT
2	Minimale lengte van het wachtwoord	14 karakters
3	Maximale lengte van het wachtwoord	Geen beperkingen
4	Complexiteitseisen	Geen opeenvolgende cijfers/ letters of verwijzing naar gebruiker of dienst. Minimaal 3 van de volgende 4 categorieën: hoofdletters, kleine letters, cijfers of leestekens Er staan aanwijzingen op intranet voor samenstelling van een veilig wachtwoord (Kiezen van een veilig wachtwoord (sharepoint.com)).
5	Geldigheidsduur wachtwoord	Minimaal 1 dag Maximaal 1 jaar
6	Wijziging wachtwoord door gebruiker bij eerste login	Ja
7	Geldigheid initieel wachtwoord	30 dagen
8	Hergebruik wachtwoord	Nee, wachtwoorden worden niet hergebruikt en zijn voor alle accounts per informatiesysteem en omgeving uniek

9	Gebruik controlesysteem	T.b.v. controle op elementen 2 t/m 8: indien nodig
10	Aankondiging verplichte wijziging wachtwoord door het systeem	Systeemmelding minimaal 3 dagen voor einddatum
11	Mogelijkheid wachtwoord herstellen door gebruiker	Ja, via Self Service Password Reset (SSPR)
12	Procedure initiële uitgifte van accounts en authenticatiemiddelen aan medewerkers	Persoonlijk verstrekken na identiteitsverificatie middels wettelijk identificatiemiddel of smartcard[1]
13	Procedure hernieuwde uitgifte authenticatiemiddel	Voor niet fysieke middelen: Door gebruiker via SSPR Overige middelen: Na identiteitsverificatie, door middel van een wettelijk identificatiemiddel of de smartcard. Dit kan fysiek of middels videocommunicatie
14	Procedure intrekken van het account bij uitdiensttreding	Automatisch op dag van vertrek
15	Loggen van inloggen (inclusief mislukte pogingen)	Ja
16	Maximaal aantal foutieve inlogpogingen (wachtwoord)	15 foutieve pogingen binnen 15 minuten waarna een blokkade van 15 minuten
17	Minimale lengte van de pincode	5 karakters
18	Ontgrendeling van mobiele apparatuur met pincode of biometrisch equivalent	Verplicht
19	Maximale geldigheidsduur pincode of biometrisch equivalent op mobiele apparatuur	Geen. Indien toch noodzakelijk: technisch afdwingen.
20	Maximaal aantal foutieve inlogpogingen (pincode)	5
21	Mogelijkheid pincode herstellen door gebruiker	Ja na interne authenticatie middels gebruikersnaam/wachtwoord
22	Multi Factor Authenticatie (MFA)	Verplicht bij gebruik van persoonlijke accounts
23	Grace periode voor de MFA	Intern: 4 uur Extern: Op basis van risicoanalyse
24	Geldigheidsduur tijdsgebonden eenmalig wachtwoord (TOTP)	Maximaal 60 seconden

[1] Voordat een smartcard wordt verstrekt aan een medewerker wordt deze gevraagd zich te legitimeren. Om die reden wordt ook de smartcard geaccepteerd als middel om de identiteit te controleren. (zie Zenya 054120)

Verder worden de volgende uitgangspunten gehanteerd:

[a] Inloggegevens zijn persoonsgebonden; toegang tot informatiesystemen middels het account van een ander is niet toegestaan
[b] Wachtwoorden dienen bij voorkeur te worden onthouden; ze worden niet opgeschreven of gedeeld
[c] Wachtwoorden mogen alleen worden opgeslagen in systemen die daarvoor bedoeld zijn.
[d] Een wachtwoord wordt onmiddellijk gewijzigd wanneer het vermoeden bestaat dat het achterhaald is en er wordt direct contact opgenomen met de MIT Klantenservice (74711)
[e] Men neemt de voorgeschreven beveiligingsregels in acht bij het kiezen en gebruiken van wachtwoorden

[f] Het gebruik van hetzelfde wachtwoord voor verschillende systemen of omgevingen is niet toegestaan

5.1 Persoonsgebonden accounts voor beheerders

Aanvullend op genoemde uitgangspunten gelden voor beheeraccounts de volgende aanvullende uitgangspunten:

[a] Beheerders maken gebruik van meerdere accounts: een persoonsgebonden gebruikersaccount voor reguliere activiteiten en persoonsgebonden beheeraccount(s) uitsluitend voor beheerwerkzaamheden

[b] Noodzakelijk gebruik van een beheeraccount door een externe partij wordt nauwkeurig gelogd; indien mogelijk wordt na beëindiging van de (onderhouds-)werkzaamheden direct het account geblokkeerd of het wachtwoord gewijzigd

5.2 Systeemaccounts

Aanvullend op genoemde uitgangspunten worden de volgende uitgangspunten gehanteerd:

[a] De identiteit van de verantwoordelijke voor een dergelijke IT-component en het systeemaccount dient vastgelegd te zijn

[b] Het systeemaccount moet herleidbaar zijn tot het technische proces

[c] Wachtwoorden mogen alleen worden opgeslagen in systemen die daarvoor bedoeld zijn. Toegang tot deze informatiesystemen is op basis van “need to know” en wordt periodiek gecontroleerd

[d] Door de leverancier aangemaakte wachtwoorden moeten na installatie worden gewijzigd

[e] Zogenaamde auto-logon systemen zijn voorzien van een systeemaccount, dat herleidbaar is tot een specifiek bedrijfsproces. Indien dit account toegang nodig heeft tot informatiesystemen, dan wordt hiervan registratie gemaakt in het risicomemorandum na akkoord van de systeemeigenaar/verantwoordelijke. Aan het verlenen van toestemming kunnen nadere voorwaarden worden gesteld

[f] Als een medewerker met kennis van systeemaccounts uit dienst gaat of van functie verandert, wordt het wachtwoord van desbetreffende accounts direct gewijzigd

5.3. Generieke accounts

Aanvullend op genoemde uitgangspunten worden de volgende uitgangspunten gehanteerd:

[a] Een generiek account wordt uitsluitend toegestaan als het gebruik van een persoonsgebonden account leidt tot te grote negatieve impact op de (patiënt)veiligheid of de werkbaarheid te sterk in het geding is.

[b] Patiëntveiligheid gaat te allen tijde boven informatieveiligheid.

[c] De systeemeigenaar dient toestemming te verlenen voor het gebruik van een generiek gebruikersaccount. Registratie hiervan vindt plaats in het risicomemorandum. Aan het verlenen van toestemming kunnen nadere voorwaarden worden gesteld

[d] Een lijnmanager is verantwoordelijk voor het gebruik van een niet-persoonsgebonden generiek gebruikersaccount

[e] Het bestaan van een generiek account wordt periodiek (minimaal 1x per jaar) door de systeemeigenaar geëvalueerd

[f] Standaardwachtwoorden zijn niet toegestaan; wachtwoorden van generieke beheeraccounts worden bij installatie gewijzigd

[g] Als een medewerker met kennis van niet-persoonsgebonden accounts uit dienst gaat of van functie verandert, wordt het wachtwoord van desbetreffende accounts direct gewijzigd

5.4. API-accounts

Aanvullend op genoemde uitgangspunten worden de volgende uitgangspunten gehanteerd:

[a] Het API-account moet herleidbaar zijn tot het technische proces.
[b] Standaard, of door de leverancier aangemaakte wachtwoorden / tokens moeten na installatie worden gewijzigd.
[c] Indien mogelijk worden standaard accountnamen bij installatie gewijzigd.
[e] Gebruik van een API-account wordt beperkt op basis van het least priveledge principe, zodat het account bijvoorbeeld alleen te gebruiken is vanaf bepaalde IP-adressen (whitelisting) of alleen op bepaalde tijdstippen in combinatie met rol gebaseerde toegangscontrole (RBAC).
[f] Zorg ervoor dat API tokens, accounts, wachtwoorden niet hardcoded in systemen wordt geplaatst.
[g] Zorg ervoor dat bij data in transit tokens, accounts, wachtwoorden altijd versleuteld worden verstuurd.
[h] Zorg ervoor de login tokens / wachtwoorden vanuit een API tijdig routeren. Routeer deze binnen 365 dagen.
[i] Houd login tokens / wachtwoorden uit de clientzijde. Gebruik server-side proxy's, token-gebaseerde authenticatie en mTLS.
[j] Plan voor snelle token / wachtwoord verwijdering. Automatiseerde dit via scripts voor noodgevallen. Hierdoor kan toegang snel ontzegd worden.
[k] Controleer regelmatig het token of wachtwoord gebruik. Kijk of sleutels nog in gebruik zijn, indien niet kunnen deze verwijderd worden, waardoor de toegang wordt ontzegd.

5.5. Break glass user accounts

Aanvullend op genoemde uitgangspunten worden de volgende uitgangspunten gehanteerd:

[a] Het break glass user account moet herleidbaar zijn tot het technische proces.
[b] Wachtwoorden voor super-user accounts moeten bij voorkeur veilig en offline (papier, kluis, digitale kluis etc.) opgeslagen worden, zodat toegang mogelijk is in gevallen dat geautomatiseerde systemen voor wachtwoord opslag niet toegankelijk zijn.
[c] Toegang tot break glass accounts en bijbehorende wachtwoorden is alleen mogelijk na het doorlopen van de betreffende noodprocedures welke is opgesteld door de beheerder of leverancier.
[d] Na gebruik van het break glass account wordt direct het wachtwoord van het account gewijzigd, op de juiste manier het wachtwoord opgeslagen en de noodzaak van toegang en activiteiten geëvalueerd.

5.6 Systemen voor wachtwoordbeheer

[a] Systemen voor wachtwoordbeheer moeten interactief zijn en sterke wachtwoorden waarborgen (ISO27002|A.9.4.3)
[b] De identiteit van de gebruiker is onveranderd door de systemen heen (non-repudiation)
[c] Het systeem dient op basis van codes gebruikers uniek te identificeren en authentiseren
[d] Identificatie en authenticatie vindt plaats op basis van actuele gegevens en vóór (vervolg) interactie met het systeem
[e] Gebeurtenissen met betrekking tot de authenticatie van gebruikers worden gelogd
[f] Waar mogelijk dwingt het informatiesysteem de eisen aan wachtwoorden af
[g] Na 20 minuten geen gebruik is her-authenticatie vereist, bijvoorbeeld door middel van een screensaver of een idle-timeout

5.7. Processen voor wachtwoordbeheer en beheer van authenticatiemiddelen

[a] Er zijn formele procedures voor het instellen, verstrekken, wijzigen en intrekken van authenticatiemiddelen vastgesteld.
[b] Authenticatiemiddelen worden als volgt verstrekt:
1) Gebruikersnaam en wachtwoord: persoonlijk aan de medewerker na identificatie
2) Fysieke authenticatiemiddelen: persoonlijk aan de medewerker na identificatie
3) Logische authenticatiemiddelen: registratie door de medewerker zelf, alleen vanaf het interne netwerk, binnen de muren van het MUMC+ en na succesvolle authenticatie.
[c] Wanner fysiek contact niet mogelijk is, worden in formele procedures de alternatieve werkwijze beschreven.
[d] Gebruikers kunnen zelf hun wachtwoord wijzigen; hierbij vindt opnieuw authenticatie plaats

6. VERANTWOORDELIJKHEDEN

De verantwoordelijkheden t.a.v. het wachtwoordbeleid zijn als volgt verdeeld:

- Medewerker: naleving van het wachtwoordbeleid
- Corporate Information Security Officer (CISO): beheer van het wachtwoordbeleid
- MIT / Functioneel beheer: implementatie wachtwoordbeleid; inrichten procedures voor verstrekken, instellen, wijzigen en intrekken van authenticatiemiddelen

7. CONTROLE EN RAPPORTAGE

- De systeemeigenaar is verantwoordelijk voor naleving van het wachtwoordbeleid.
- De CISO is verantwoordelijk voor toezicht op de naleving van het wachtwoordbeleid.
- Onafhankelijke controle op de naleving van het wachtwoordbeleid valt onder de verantwoordelijkheid van de auditfunctie (intern en extern). Hierover wordt gerapporteerd aan alle bij de controle betrokken functionarissen en instanties.

8. DOCUMENTATIE

Bij deze richtlijn horen:

1. Reglement omgang met Informatie en IT-middelen van MUMC+ | Zenya 003486; Artikel 2 Lid 3
2. Intranet | Richtlijn voor gebrukers | Kiezen van een veilig wachtwoord | Kiezen van een veilig wachtwoord (sharepoint.com)
3. De relevante procedures en formulieren van MIT-Klantenservice

9. BRONNEN

1. SIG-IB Architectuur Bouwblok Authenticatie v1.0, kader voor toegangsbeleid NFU breed
2. NEN7510 /11
3. ISO27002 Praktijkrichtlijn met beheersmaatregelen op het gebied van informatiebeveiliging: Annex 9.3.1
4. Digital Identity Guidelines; Authentication and Lifecycle Management; special publication 800-63B van het National Institute of Standards and Technology (NIST)
5. Best practices: inventarisatie van de password policies van andere UMC’s