Autorisatie en authenticatie beleid mboRijnland

Boek 9 IBP, hoofdstuk 9 van ISO27002

Versiebeheer

Versie	Status	Datum	Auteur	Omschrijving
0.1	Concept	11-7-2019	Ludo Cuijpers	1e Draft, mede op basis van Autorisatie en authenticatie beleid mboRijnland
0.2	Concept	11-7-2019	Vincent Reijnen en Ludo Cuijpers	Aanpassen processen mboRijnland
0.5	Concept	6-8-2019	Niels Dutij, Ludo Cuijpers, Vincent Reijnen	2e Draft (applicatie eigenaar SIS benoemd), nummering aangepast aan hoofdstuk 9 ISO en MFA verwijderd.
0.6	Concept	10-9-2019	Ludo Cuijpers, Vincent Reijnen	Slot draft
1.0	Definitief	8-11-2019	Vincent Reijnen	Slot draft vastgesteld

Inhoud

9.1.1 BELEID VOOR TOEGANGSBEVEILIGING (TK 5.1)

Dit document beschrijft het informatiebeveiligingsbeleid voor toegangsbeveiliging, gebaseerd op ISO27002:2013. Dit betekent dat regels ten aanzien van informatiebeveiliging worden opgesteld gebaseerd op de al eerder genoemde vooronderstelling “Alles is in principe verboden tenzij het uitdrukkelijk is toegelaten” in plaats van de zwakkere regel “Alles is in principe toegelaten tenzij het uitdrukkelijk is verboden”.
Beleidsplan 1.7 punt 15 *Governance, 1st line of defense*

9.1.2 TOEGANG TOT NETWERKEN EN SYSTEMEN (TK 5.2)

Gebruikers behoren alleen toegang te krijgen tot het netwerk en de systemen of delen van systemen waarvoor zij specifiek bevoegd zijn. Uitgangspunt voor het verlenen van toegang tot systemen is het “need-to-know[1]” en/of “need-to-use” principe. Afhankelijk van de rol of taak van de gebruiker worden autorisaties voor toegang tot gegevens en/of systemen toegekend door de beheerder in opdracht van de leidinggevende.
De principes “need-to-know” en “need-to-use” gelden voor alle gebruikers en typen gebruikersaccounts.
Bovendien hanteert mboRijnland het “least privilege” principe, dus er worden alleen rechten toegekend aan medewerkers als dat strikt noodzakelijk is.
De systeemeigenaar (applicatie eigenaar) voor het HRM Systeem is verantwoordelijk voor het opzetten en onderhouden van de autorisatiematrix. Voor mboRijnland is de systeemeigenaar voor het HRM Systeem de directeur SSC Administraties.
Het “least privilege” principe wordt getoetst door de FG’er in het kader van dataminimalisatie.
Het “least privilege” principe wordt ook getoetst door de controller of accountant in het kader van “Segregation of duties”, waardoor medewerkers geen combinatie van rechten kunnen hebben waardoor fraude mogelijk is (facturen uitschrijven en innen).
Beleidsplan 3.5, autorisaties, *3th line op defense*

9.2.1 REGISTRATIE EN AFMELDEN VAN GEBRUIKERS (TK 5.3)

Om er voor te zorgen dat alleen bevoegde gebruikers toegang verkrijgen tot de voor hun werkzaamheden (inclusief studieactiviteiten van studenten) benodigde netwerken en systemen dient een proces voor instroom, doorstroom en uitstroom (IDU proces) te zijn ingericht. Binnen het IDU proces moeten de basis autorisaties aan gebruikers worden toegekend. Extra autorisaties worden door de leidinggevenden toegekend.

Gebruikers krijgen een uniek gebruikersaccount. Binnen het IDU proces worden gebruikersaccounts en de benodigde rollen geactiveerd en gedeactiveerd op het juiste moment. Het is mogelijk dat gebruikers meerdere rollen binnen de onderwijsorganisatie vervullen, deze worden allen gekoppeld aan één account. Bij het uit dienst treden, beëindigen van de studie of anderszins volledig beëindigen van de relatie met de onderwijsinstelling wordt het aan de betreffende gebruiker toegekende account in onmiddellijk gedeactiveerd. Dit geldt voor alle gebruikers met een account.

Het is gebruikers uitdrukkelijk verboden om hun persoonlijke gebruikersaccount en wachtwoord met anderen te delen. Dit is ook expliciet vermeld in het “Reglement verantwoord gebruik ICT-faciliteiten medewerkers”.
Reglement verantwoord gebruik ICT-faciliteiten medewerkers, Artikel 3. Gebruik van computer- en netwerkfaciliteiten, *3.2. De medewerker dient te allen tijde zorgvuldig om te gaan met aan hem persoonlijk toegekende inloggegevens en eventuele aanvullende authenticatiemiddelen (zoals smartcards en tokens). Persoonsgebonden wachtwoorden en aanvullende authenticatiemiddelen mogen niet worden gedeeld. Bij een vermoeden van misbruik van een account is de afdeling ICT geautoriseerd per direct het betrokken account ontoegankelijk te maken en de rechten op het gebruik van het netwerk van de medewerker in te trekken.*

[1] Personen krijgen alleen toegang tot functies en informatie voor zover dit strikt noodzakelijk is voor het uitvoeren van de aan hen opgedragen werkzaamheden.

9.2.2 GEBRUIKERS TOEGANG VERLENEN (TK 5.4)

Gebruikers krijgen bij de aanmaak van hun account toegang tot een data en persoonsgegevens binnen het netwerk, zoals:

- De aan hun gebruikersaccount gekoppelde OneDrive voor persoonlijk gegevensopslag;
- De groepsomgeving (bijvoorbeeld OneDrive voor een team) van de afdeling(en) waarbij de gebruiker organisatorisch is ingedeeld;.
- De persoonlijke e-mail box;
- Etc.

Voor toegang tot andere onderdelen van het netwerk of andere systemen is een aanvraagprocedure / proces ingericht met goedkeuring van de leidinggevende. De leidinggevenden zien er op toe en zijn verantwoordelijk voor het toekennen van de juiste autorisatie voor toegang tot netwerkonderdelen en systemen.

De leidinggevende is verantwoordelijk voor:

- Het periodiek verifiëren dat de in de autorisatiematrix gedefinieerde autorisaties in overeenstemming zijn met de beleidsregels voor toegang, zoals in dit document vastgelegd, en consistent zijn met andere eisen zoals functiescheiding en “need-to-know”. Het resultaat wordt vastgelegd in een verslag van bevindingen, dat wordt gearchiveerd;
- waarborgen dat autorisaties niet worden geactiveerd voordat de autorisatieprocedures zijn afgerond;
- bijhouden van een overzicht per organisatorische eenheid van aanvullende autorisaties uit de autorisatiematrix die aan de gebruikersaccounts, van de aan de leidinggevende toegewezen medewerkers, zijn toegekend, de zogenaamde SOLL autorisatie matrix;
- aanpassen van autorisaties van gebruikers van wie de rollen of functies zijn gewijzigd en autorisaties van gebruikers die de organisatie hebben verlaten onmiddellijk verwijderen of blokkeren. Het is hiervoor noodzakelijk dat de systeemeigenaren vanuit het IDU proces worden getriggerd;
- het periodiek beoordelen van autorisaties door de SOLL autorisatie matrix te vergelijken met de IST autorisatiematrix. Deze IST autorisatiematrix wordt opgeleverd door de applicatie of functioneel beheerders.

Bijzondere aandacht vereist het proces van functiewijzigingen (“Doorstroom”) en de daarbij behorende verandering van benodigde autorisaties. Alle niet meer benodigde autorisaties dienen te worden ingetrokken. De eenvoudigste manier om dit goed te regelen is in de aanvraag voor autorisatie voor de nieuwe functie alle benodigde autorisaties op te nemen en alle oude autorisaties te laten vervallen, indien mogelijk door tussenkomst van IDM.
Geen verdere verwijzing. In toetsingskader staat dan zie 5.4 uit BOEK 9 IBP.

9.2.3 BEHEREN VAN SPECIALE TOEGANGSRECHTEN[2] (TK 5.5)

Speciale toegangsrechten zijn bijvoorbeeld toegang tot operating systemen, databases en beheeraccounts van toepassingssystemen. Ook standaard bij applicaties en systemen geïnstalleerde accounts (out of the box), veelal met hoge rechten, vallen in deze categorie[3].

Voor accounts met speciale rechten gelden de volgende uitgangspunten:

- De speciale toegangsrechten van ieder systeem en elke toepassing (inclusief beheeraccounts van netwerkapparatuur etc.) en de gebruikers aan wie ze moeten worden toegewezen moeten worden geïdentificeerd en geregistreerd;
- Speciale toegangsrechten worden alleen op basis van “need-to-know” en “need-to-use” toegekend;
- Voor de toekenning van speciale toegangsrechten is een proces ingericht, waarbij de leidinggevende gebruikers expliciet autoriseert voor de benodigde speciale rechten. Deze expliciete autorisatieaanvraag wordt gearchiveerd;
- Speciale rechten worden nooit toegekend aan een standaard gebruikersaccount voor dagelijkse werkzaamheden (mail, tekstverwerking, spreadsheet, etc.), ;
- Accounts met speciale rechten, toegekend aan gebruikers, worden bij vertrek of functiewijziging onmiddellijk geblokkeerd en verwijderd;
- Leidinggevende evalueren periodiek (elke drie maanden) de accounts met speciale rechten en verwijderen accounts met speciale rechten die niet langer benodigd zijn. Het resultaat wordt vastgelegd in een verslag van bevindingen, dat wordt gearchiveerd;
- Activiteiten van accounts met speciale rechten worden gelogd.

Geen verdere verwijzing. Evidence in toetsingskader 4.0: zie 5.5 uit BOEK 9 IBP.

9.2.4 BEHEER VAN GEHEIME AUTHENTICATIE-INFORMATIE (WACHTWOORDEN) VAN GEBRUIKERS (TK 5.6)[4]

Voor het verlenen van de toegang tot netwerken en applicaties maakt de onderwijsinstelling gebruik van gebruikersnamen en wachtwoorden. Dit betekent dat wachtwoorden een belangrijk aspect vormen van de informatiebeveiliging. Het is dan ook zaak dat de gebruikers van de onderwijsinstelling goede wachtwoorden kiezen, waarmee de kans op onterechte toegang en mogelijk onrechtmatig gebruik, verwijdering of manipulatie van gegevens wordt voorkomen. Het gaat daarbij bijvoorbeeld om gegevens rond de bedrijfsvoering, HR-processen en studentenadministratie.

Dit betekent dat er naast een goede omgang met wachtwoorden door gebruikers en goede processen procedures rond het wachtwoordbeheer en het toekennen en intrekken van autorisaties zijn opgesteld. Dit geldt voor alle gebruikers van de onderwijsinstelling.

De belangrijkste maatregelen voor alle gebruikers van de onderwijsinstelling zijn het kiezen van wachtwoorden die moeilijk te “kraken” zijn (sterke wachtwoorden) en dat zij deze **niet delen met anderen**, maar deze geheimhouden. Het sterke wachtwoord wordt afgedwongen bij het aanmaken en wijzigen van het wachtwoord.

“Gewone” gebruikersaccounts voor medewerkers, en studenten”, worden in een geautomatiseerd proces via IDM (IDentity Management), gegenereerd. Bij de eerste keer inloggen moet de gebruiker het initiële wachtwoord wijzigen.

Speciale toegangsrechten worden door middel van een formulier bij de leidinggevende aangevraagd en na diens goedkeuring door de beheerders aangemaakt.

---

[2] Medewerkers met de hoogste rechten, waardoor zij bijvoorbeeld alles kunnen inzien, verwijderen, etc.

[3] Voorbeelden van dit type accounts zijn:
- Windows: Azure, AD, O365 : SYSADM, ADMIN
- Linux/Unix: Root
- SAP: SAP*, DDIC, SAPCPIC en EARLYWATCH

[4] Zie bijlage 1: Wachtwoordbeleid mboRijnland

Standaard met applicaties meegeleverde accounts en wachtwoorden worden geblokkeerd. Indien dit niet mogelijk is, wordt het wachtwoord gewijzigd en op een veilige plaats opgeborgen (bijvoorbeeld: gesloten enveloppe in een kluis).

Gebruikersnaam en wachtwoord worden versleuteld opgeslagen. Ook het transport van gebruikersnaam en wachtwoord over het netwerk c.q. naar een (externe) web applicatie mag uitsluitend versleuteld gebeuren.

Authenticatievormen
De meest bekende vorm van authenticatie is het gebruik van een gebruikersnaam met een wachtwoord. Er zijn echter meer authenticatievormen, die ook in combinatie kunnen worden gebruikt. Een opsomming:

1. **“Je weet wat”**
   Dit is de meest voorkomende vorm van authenticatie, bijvoorbeeld een pincode, wachtwoord of wachtwoordzin (passphrase).
2. **“Je hebt wat”**
   Bij deze vorm van authenticatie moet je in het bezit zijn van iets, waarmee je kunt aantonen dat degene bent die bij de gebruikersnaam hoort. Dit kan in de vorm van een smartcard die je in een lezer moet stoppen, of een token dat een code genereert die je handmatig moet invoeren.
3. **“Je bent wat”**
   Op basis van biometrische eigenschappen wordt je geauthentiseerd, Voorbeelden daarvan zijn de irisscan, vingerafdruk, of stemherkenning.

Door combinatie van meerdere authenticatiemethoden kan de toegangsbeveiliging worden versterkt. In dat geval wordt er gesproken over multi-factor authenticatie (MFA).

Daar waar hoge eisen worden gesteld aan de beveiliging van systemen en toepassingen zal de onderwijsinstelling multi-factor authenticatie toepassen. De criteria daarvoor zijn gebaseerd op dataclassificatie. Bij een Vertrouwelijkheid van Midden of Hoog wordt altijd MFA toegepast.
Geen verdere verwijzing. In toetsingskader staat dan zie 5.6 uit BOEK 9 IBP.

9.2.5 BEOORDELING VAN TOEGANGSRECHTEN VAN GEBRUIKERS (TK 6.1)

De leidinggevende dienen periodiek de toegangsrechten van alle gebruikers te evalueren (SOLL en IST matrix) en daar waar nodig in te trekken of te corrigeren. Het resultaat van de periodieke controle wordt vastgelegd in een verslag van bevindingen, dat wordt gearchiveerd. Alhoewel al eerder in diverse paragrafen genoemd, wordt deze beheersmaatregel hier nogmaals expliciet neergezet. mboRijnland hanteert een bewaartermijn van 2 jaar voor het verslag van de bevindingen.
Geen verdere verwijzing. In toetsingskader staat dan zie 6.1 uit BOEK 9 IBP.
Het is wenselijk om een format lijst toe te voegen waarin leidinggevenden aangeven aan wie zij welke rechten hebben toegekend.

9.2.6 TOEGANGSRECHTEN INTREKKEN OF AANPASSEN (TK 2.3)

De toegangsrechten van alle medewerkers en externe gebruikers voor het netwerk en de diverse toepassingen behoren bij beëindiging van hun dienstverband, contract of overeenkomst te worden verwijderd, en bij wijzigingen behoren ze te worden aangepast.

Ingeval de directie de beëindiging van het dienstverband, contract of overeenkomst heeft geïnitieerd bestaat het risico dat misnoegde medewerkers of externe gebruikers opzettelijk informatie corrumperen of systemen saboteren. Personen waarvan het dienstverband eindigt kunnen in de verleiding komen informatie te verzamelen voor toekomstig gebruik. In dergelijke gevallen worden alle accounts worden persoonlijke accounts onmiddellijk geblokkeerd. De vertrekkende persoon wordt in voorkomend geval nog expliciet op de geheimhoudingsverklaring gewezen.
Geen verdere verwijzing. In toetsingskader staat dan zie 2.3 uit BOEK 9 IBP.

9.3.1 GEHEIME AUTHENTICATIE-INFORMATIE GEBRUIKEN (TK 5.7)

Afhankelijk van de dataclassificatie uit de dataregisters worden eisen aan geheime authenticatie informatie (wachtwoorden, eventueel ook de tweede factor bij two-factor authenticatie) gesteld. Over het algemeen geldt dat er gebruik gemaakt wordt van “sterke wachtwoorden”.

Een aantal algemene eisen ten aanzien wachtwoorden:

- Van gebruikers wordt verlangd dat zij hun inloggegevens geheimhouden conform het “Reglement verantwoord gebruik ICT-faciliteiten medewerkers”.
- Gebruikers registreren geen geheime inloggegevens (bijv. op papier, in een computerbestand of op een zakapparaat), tenzij deze informatie veilig kan worden opgeslagen en de opslagmethode is goedgekeurd door de afdeling ICT.
- Geheime authenticatie-informatie wordt onmiddellijk gewijzigd als er een aanwijzing is dat deze mogelijk is gecompromitteerd.
- Zorg voor passende bescherming van wachtwoorden wanneer wachtwoorden worden gebruikt als geheime authenticatie-informatie in geautomatiseerde inlogprocedures en in/bij de procedure worden opgeslagen.

Als ‘Single Sign On’ (SSO) of andere beheerinstrumenten voor eenmalig aanmelden beschikbaar worden gesteld vermindert dat de hoeveelheid wachtwoorden die gebruikers moeten beschermen, waardoor de doeltreffendheid van deze beheersmaatregel kan toenemen. Echter, deze instrumenten kunnen ook de impact van het bekend worden van wachtwoorden vergroten.
Geen verdere verwijzing. In toetsingskader staat dan zie 5.7 uit BOEK 9 IBP.

9.4.1 BEPERKING TOEGANG TOT INFORMATIE (TK 5.8)

Voor het beschermen van gegevens in systemen en toepassingen dienen toegangsbeperkingen te worden ingericht. Zoals eerder opgemerkt: autorisatie van gebruikers vindt plaats op basis van “need-to-know” en/of “need-to-use”. Het beveiligingsniveau wordt aangepast op de gevoeligheid van de gegevens en systemen. Dit gebeurt op basis van de dataclassificatie.
Geen verdere verwijzing. In toetsingskader staat dan zie 5.8 uit BOEK 9 IBP.

9.4.2 BEVEILIGDE INLOGPROCEDURES (TK 5.9)

Alle netwerken en systemen van de onderwijsinstelling zijn slechts toegankelijk via een beveiligde inlogprocedure. Dit betekent dat gebruikersnaam en wachtwoord altijd via een beveiligde verbinding worden verstuurd, zodat onderscheppen door middel van “sniffing[5]” erg moeilijk dan wel zelfs onmogelijk is.

Daarnaast geldt de verplichting om MFA te gebruiken bij systemen die persoonsgegevens verwerken met de vertrouwelijkheid classificatie Midden of Hoog.

Een goede inlogprocedure omvat de volgende maatregelen:

- Een algemene waarschuwing tonen dat de computer alleen toegankelijk is voor bevoegde gebruikers;
- Het tonen van de laatste ingelogde gebruikersnaam is niet toegestaan;
- Tijdens de inlogprocedure geen hulpboodschappen weergeven waarmee onbevoegde gebruikers hun doel kunnen bereiken;
- De inloginformatie pas na invoer van alle gegevens valideren. Indien zich een fout voordoet, behoort het systeem niet aan te geven welk deel van de gegevens juist of onjuist is;
- Bescherming bieden tegen inlogpogingen die met grove middelen worden uitgevoerd (Brute Force Attack);
- Niet-succesvolle en succesvolle inlogpogingen worden geregistreerd in een logbestand (NB: Niet de wachtwoorden), bewaartermijn 6 maanden;
- Bij een poging tot of een succesvolle schending van de inlogbeheersmaatregelen wordt een informatiebeveiligingsincident geïnitieerd;
- Een wachtwoord dat wordt ingevoerd wordt niet leesbaar weergegeven;
- Inactieve sessies van toepassingen worden na een bepaalde tijd van inactiviteit van de gebruiker beëindigd.

Geen verdere verwijzing. In toetsingskader staat dan zie 5.9 uit BOEK 9 IBP.

9.4.3 SYSTEEM VOOR WACHTWOORDBEHEER (TK 5.18)

Indien een systeem voor wachtwoordbeheer wordt toegepast, dienen onderstaande eisen te worden gehanteerd. De eisen aan een dergelijk systeem worden ook gesteld aan individuele systemen en toepassingen, voor zover er geen gebruik wordt gemaakt van SSO.

- De keuze voor sterke wachtwoorden wordt afgedwongen, de gewenste complexiteit wordt ingesteld;
- Gebruikers hebben de mogelijkheid hun eigen wachtwoord te kiezen en te wijzigen binnen de gestelde complexiteitseisen;
- Gebruikers worden gedwongen hun initiële wachtwoord bij het eerste inloggen te wijzigen;
- Periodieke wijziging van het wachtwoord wordt afgedwongen;
- Voorkomt dat wachtwoorden opnieuw worden gebruikt door een wachtwoordhistorie bij te houden;
- Wachtwoorden worden niet leesbaar op het scherm getoond als ze worden ingevoerd;
- Wachtwoordbestanden worden apart van systeemgegevens van toepassingen opgeslagen;
- Wachtwoorden worden versleuteld opgeslagen en verstuurd.

Alle applicaties en toepassingen binnen de onderwijsinstelling worden zodanig ingericht dat, voor zover technisch mogelijk, aan de bovenstaande eisen wordt voldaan.
Geen verdere verwijzing. In toetsingskader staat dan zie 5.18 uit BOEK 9 IBP.

[5] Sniffing is het aftappen of meeluisteren van informatiestromen in het netwerk om daarmee de gegevens (in dit geval gebruikers ID en wachtwoord) te onderscheppen. Als de inhoud van de gegevensstroom is versleuteld is het veel moeilijker om de inloggegevens te onderscheppen.

9.4.4 SPECIALE SYSTEEMHULPMIDDELEN GEBRUIKEN (TK 5.19)

Hulpmiddelen (tools) voor het uitvoeren van beheertaken zijn vaak in staat om beheersmaatregelen, zoals toegangsbeveiliging, voor systemen en toepassingen te omzeilen. Dit betekent dat bij de inzet van deze hulpmiddelen een aantal richtlijnen noodzakelijk is, die, voor zover technisch mogelijk, worden afgedwongen:

- gebruik van identificatie-, authenticatie- en autorisatieprocedures voor systeemhulpmiddelen;
- systeemhulpmiddelen en toepassingssoftware worden in principe van elkaar gescheiden. Daar waar systeemhulpmiddelen noodzakelijk zijn voor monitoring/bewaking, kunnen die onderdelen van de hulpmiddelen die daarvoor noodzakelijk zijn, toch worden ingezet;
- het gebruik van systeemhulpmiddelen wordt beperkt tot het laagste aantal betrouwbare bevoegde gebruikers dat praktisch haalbaar is, hierbij kan ook gebruik worden gemaakt van ad-hoc en in tijd beperkte autorisatie voor het gebruik;
- registreren (logging) van alle gebruik van systeemhulpmiddelen;
- verwijderen of onbruikbaar maken van alle onnodige systeemhulpmiddelen;
- niet beschikbaar stellen van systeemhulpmiddelen aan gebruikers die toegang hebben tot toepassingen op systemen waarbij scheiding van taken vereist is.

Geen verdere verwijzing. In toetsingskader staat dan zie 5.19 uit BOEK 9 IBP.

9.4.5 TOEGANGSBEVEILIGING OP PROGRAMMABRONCODE (TK 5.20)

Toegang tot programmabroncodes en samenhangende items (zoals ontwerpen, specificaties, verificatie- en validatieschema's) behoort strikt te worden beheerst om de introductie van onbevoegde functionaliteit en om onbedoelde wijzigingen in de productieomgeving te voorkomen, alsmede om de vertrouwelijkheid van waardevolle intellectuele eigendom te handhaven. In veel gevallen kunnen de maatregelen die gelden voor het beheersen van de vertrouwelijke gegevens op basis van de BIV classificatie worden gehanteerd.

In het geval van zogenaamde "Open Source" software dienen de bijbehorende licentievoorwaarden in acht te worden genomen en is de alinea hierboven niet van toepassing.

Met betrekking tot de programmabroncode kan een goede beheersing van de toegang worden bereikt door de code gecontroleerd centraal op te slaan, bij voorkeur in de broncodebibliotheek met geautomatiseerd versiebeheer.

Geen verdere verwijzing. In toetsingskader staat dan zie 5.20 uit BOEK 9 IBP.

Bijlage 1: Wachtwoordbeleid mboRijnland

Wachtwoorden in de ICT infrastructuur en applicaties worden gehandhaafd op basis van de volgende principes:

Wachtwoord historie
- Het wachtwoord mag de laatste 24 keer niet als wachtwoord gebruikt zijn.

Maximum geldigheid wachtwoord
- Een wachtwoord is 180 dagen geldig, daarna dient een nieuw wachtwoord ingesteld te worden.

Minimum geldigheid wachtwoord
- Een wachtwoord mag niet te snel, pas na 2 dagen, worden aangepast. Dit is om te voorkomen dat er snel 24 nieuwe wachtwoorden worden ingesteld om de wachtwoordhistorie te omzeilen.

Minimum lengte wachtwoord
- Een wachtwoord is minimaal 9 karakters lang.

Wachtwoord dient complex te zijn
- Een wachtwoord dient minimaal drie van de vier onderstaande groepen te bevatten:
    - Hoofdletters (A – Z);
    - Kleine letters (a – z);
    - Getal (1 – 9);
    - Niet alfanumeriek (bijvoorbeeld: !, $, #, %;

Daarnaast is een wachtwoord:
- Niet de gebruikersnaam;
- Bij voorkeur een lange makkelijk te onthouden zin.