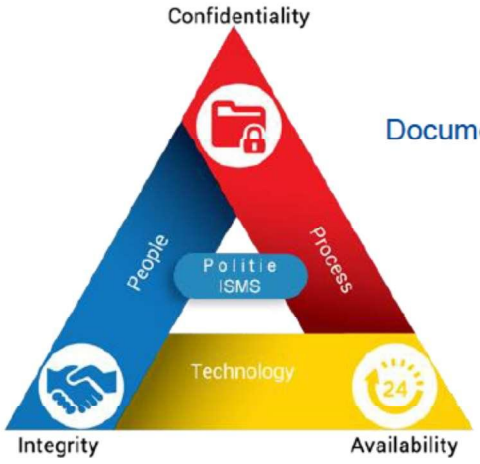
POLITIE

Wachtwoordbeleid

2022



Document referentienummer:	ISMS-A09.03.01-01
Document auteur:	5.1.2.e
Document eigenaar:	5.1.2.e
Status:	Definitief
Versie nummer:	2.0
Versie datum:	2 augustus 2022
Geldigheidsduur:	2 jaar na ondertekening
Rubricering:	Pol. INTERN

« waakzaam en dienstbaar »

Documentinformatie

Document referentienummer:	ISMS-A09.03.01-01
Document auteur:	5.1.2.e
Document eigenaar:	5.1.2.e
Status:	Definitief
Versie nummer:	2.0
Versie datum:	2 augustus 2022
Geldigheidsduur	2 jaar na ondertekening
Rubricering:	Pol. INTERN
Documentnaam	ISMS-A09.03.01-01-Wachtwoordbeleid 2022.docx

Deze tabel vult automatisch

Deze versie vervangt alle voorgaande versies van dit document.

Accordering

Naam	Functie	Handtekening	Datum
5.1.2.e	5.1.2.e	5.1.2.e	10-9-2022

Distributielijst

Versie	Datum	Verspreidingsvorm	Naam/Functie/Opmerking
1.90	13-07-2022	Digitaal	IB Risicomanagement en IB-beleid
1.98	02-08-2022	Digitaal	Security tafel ter goedkeuring
2.0			Na Goedkeuring

Reviews

Versie	Datum	Door	Functie
1.90	15-07-22	5.1.2.e	Beleidsadviseur Informatiebeveiliging
1.90	14-07-22	5.1.2.e	Kwartiermaker Cluster Beleid & Regie
1.90	14-07-22	5.1.2.e	Beleidsadviseur Informatiebeveiliging
1.90	14-07-22	5.1.2.e	Cluster Risk Management

Versiegeschiedenis

Versie	Datum	Door	Opmerkingen
1.0	Jan. 2020	5.1.2.e	Vorige versie Wachtwoordbeleid
1.90	Juli 2022	5.1.2.e	Voorstel nieuwe versie
1.98	02-08-2022	5.1.2.e	Commentaar verwerkt, lay-out aangepast
2.0		5.1.2.e	Vastgesteld
2.0		Beleidstafel IV	Vastgesteld

Bijbehorende documenten

Versie	Datum	Omschrijving

Voorwoord

De frequentie en impact van cyberaanvallen op bedrijven en overheden nemen toe[1] en hackers hebben steeds slimmere manieren om malware binnen te brengen of inlog-informatie afhandig te maken. Hogere rekenkracht van computers maken het achterhalen van een wachtwoord steeds eenvoudiger. Dit wachtwoordbeleid is grotendeels hetzelfde als het vorige wachtwoordbeleid maar er wordt meer nadruk gelegd op lange wachtwoorden (wachtzinnen) en het sluit aan bij wat de NIST en het NCSC recent gepubliceerd hebben op het gebied van wachtwoorden en inzichten. Tijdens de Cyber Security Taskforce in 2018 is al besloten door de dienstleiding van de Dienst ICT dat een wachtwoord alleen niet meer voldoende veilig is in deze tijd en dat we naar 2-factor (of Multifactor) Authenticatie moeten over gaan. 5.1.2.i . In combinatie met Multifactor Authenticatie hoeft een wachtwoord niet heel lang te zijn en kan de geldigheidsduur langer worden gemaakt. Het belang van een juiste Identificatie en Authenticatie neemt alleen maar toe door Single Sign On en Cloud gebruik. We moeten dus naar een beter, veiliger toegangssysteem van onze ICT toe.
Hoe dit concreet uitwerkt in het wachtwoordbeleid staat verderop in dit document beschreven.

[1] https://www.nctv.nl/documenten/publicaties/2022/07/04/cybersecuritybeeld-nederland-2022 en ook https://www.rathenau.nl/nl/digitale-samenleving/een-nooit-gelopen-race

Inhoudsopgave

1. Inleiding

Aanscherping kaders
De Politie heeft besloten de BIO (Baseline Informatiebeveiliging Overheden) te hanteren en dan is het goed om te kijken hoe het al bestaande wachtwoordbeleid in lijn gebracht kan worden (op basis van een risicoafweging) met de BIO. Dit heeft geleid tot een aanscherping van de kaders die de rijksoverheid gebruikt (BIO, zie fig. 1) en “de facto” wereldwijde standaarden zoals bijv. zijn vastgelegd in de NIST-800-63.

9.4.3	1	**Systeem voor wachtwoordbeheer** Systemen voor wachtwoordbeheer behoren interactief te zijn en sterke wachtwoorden te waarborgen.
9.4.3.1	1	Als er geen gebruik wordt gemaakt van two factor authentication is de wachtwoordlengte minimaal 8 posities en complex van samenstelling. Vanaf een wachtwoordlengte van 20 posities vervalt de complexiteitseis. Het aantal inlogpogingen is maximaal 10. De tijdsduur dat een account wordt geblokkeerd na overschrijding van het aantal keer foutief inloggen is vastgelegd.
9.4.3.2	2	In situaties waar geen two-factor authenticatie mogelijk is, wordt minimaal

B.

Figuur 1. Nieuwe standaarden BIO

Aanpassen wachtwoordbeleid
Wachtwoorden-wachtzinnen bij politie bestaan nu vaak uit 5.1.2.i maar moeten naar 5.1.2.i, en het wachtwoordbeleid is daarop aangepast.
Daarnaast heeft het oude principe van gebruikersnaam/ wachtwoord zijn langste tijd gehad; we moeten naar een sterkere authenticatie toe. De beste manier hiervoor is het toevoegen van een tweede factor zodat je toegang kunt verkrijgen met iets dat je **weet** (gebruikersnaam en wachtwoord) en iets wat je **hebt** (token, toegangspasje of smartphone) of iets wat je **bent** (biometrische kenmerken zoals vingerafdruk, irisscan, gezichtsscan, oid.).

2. Toepassingsgebied

De gehele ICT van de Politie.

3. Doelen

Deze nieuwe versie van het wachtwoordbeleid is niet erg afwijkend van de vorige versie, wel een aantal zaken aangepast naar aanleiding van de veranderende inzichten.
Het onderstaande herzien beleid is gebaseerd op de huidige versie van de BIO met een aantal aanscherpingen vanuit NIST en het NCSC[2] om aan te sluiten bij de actuele eisen rond wachtwoorden/wachtzinnen. Het belangrijkste verschil tussen het actuele en het oude beleid is weergegeven in de onderstaande tabel.

Actueel wachtwoordbeleid	**Oud beleid**	
*Politie intern **en** politie confidentieel*	*Politie intern*	*Politie confidentieel*
5.1.2.i **of** 5.1.2.i	5.1.2.i	5.1.2.i of 5.1.2.i

Een wachtwoord of wachtzin van 5.1.2.i zal naar verwachting niet als gebruiksvriendelijk worden ervaren. Het is dus verstandig om waar mogelijk gebruik te maken van two-factor authenticatie in combinatie met “single sign on”, om hiermee de gebruiksvriendelijkheid te vergroten.

Voor het verlopen van de wachtwoorden staat in de BIO onder 9.4.3.5:
“Wachtwoorden/wachtzinnen die voldoen aan het wachtwoordbeleid, hebben een maximale geldigheidsduur van 5.1.2.i . Daar waar het beleid niet toepasbaar is, geldt een maximale geldigheidsduur 5.1.2.i .”

Met de ondertekening van dit beleid vervallen de overlappende kaders uit de BIO en oudere versies en wordt dit wachtwoord-wachtzin beleid van toepassing.

[2] https://www.ncsc.nl/onderwerpen/multifactorauthenticatie/documenten/factsheets/2019/juni/01/factsheet-gebruik-tweefactorauthenticatie

4. Principes

4.1. Algemeen

Bij het aanmelden bij informatiesystemen identificeert de gebruiker zich met zijn of haar accountnaam. De identiteit van de gebruiker wordt vervolgens vastgesteld (authenticatie) door het invoeren van een wachtwoord/wachtzin en/of door het gebruik van hard-, of soft- tokens en/of biometrie. Medewerkers (gebruikers) behoren goede beveiligingsgewoontes in acht te nemen bij het gebruik van accounts en het kiezen en gebruiken van wachtwoorden/wachtzinnen.

Dit beleid beschrijft de beveiligingseisen waaraan accounts ten aanzien van het identificatieproces moet voldoen, alsmede de eisen die aan het wachtwoord/wachtzin en het gebruik van het wachtwoord/wachtzin worden gesteld. Wachtwoord-/wachtzinlengtes van 5.1.2.i worden toegestaan evenals het gebruik van alle mogelijke karakters en leestekens. Het gebruik van de andere middelen voor authenticatie worden in deze uitvoeringsregeling buiten beschouwing gelaten.

4.2. Type accounts

De beveiligingseisen voor accounts en wachtwoorden zijn opgedeeld in drie categorieën namelijk gebruikers en functionele accounts, privileged (admin of beheer) accounts en service accounts.

4.2.1. Gebruikersaccounts

Beveiligingseisen ten aanzien van het account:

1) Iedere gebruiker identificeert zich met zijn accountnaam;
2) Iedere handeling vanuit een account is tot een natuurlijk persoon herleidbaar;
3) Iedere accountnaam is uniek;
4) Iedere gebruiker heeft 1 uniek account. Indien in de praktijk dit uitgangspunt nog niet gerealiseerd kan worden dient ten minste een zodanige inrichting plaats te vinden dat het voor eenieder helder is: “dat het één en dezelfde gebruiker betreft.”
5) Iedere beheerder heeft aanvullend op het voorgaande punt 1 uniek account voor beheeractiviteiten;
6) De accountnaam is betekenisloos en bevat dus geen gegevens over de functie, afdeling of het soort werkzaamheden van de gebruiker;
7) Het gebruikersaccount van eerder aangemelde gebruikers mag tijdens het inloggen van de volgende gebruiker niet getoond worden;
8) Authenticatie van de gebruiker vindt plaats via 5.1.2.i .

Beveiligingseisen ten aanzien van het wachtwoord/wachtzin:

1 Een wachtwoord/wachtzin dient te voldoen aan de volgende eisen:

1) Moet voor gebruikers 5.1.2.i lang zijn en een aanvullend two-factor authenticatie middel is noodzakelijk. Indien dit niet mogelijk is wordt een wachtwoord/wachtzin vereist van 5.1.2.i ;
2) Mag niet de inlognaam (accountnaam), roepnaam en/of achternaam van de gebruiker bevatten;
3) Mag niet op een blacklist staan;
4) Bevat karakters uit 5.1.2.i :
   a. hoofdletters (A t/m Z)
   b. kleine letters (a t/m z)
   c. cijfers (0 t/m 9)
   d. leestekens (bijvoorbeeld: -, !, $, #, %)
   Deze complexiteitseisen zijn niet vereist indien meer dan 5.1.2.i worden gebruikt.

2) Na het 5.1.2.i van een foutief wachtwoord/wachtzin, wordt de toegang geblokkeerd en dient reset via de Servicedesk of de wachtwoord resettool (voor KA- wachtwoord/wachtzin) plaats te vinden;
3) Na het 5.1.2.i foutief toepassen van de wachtwoord resettool wordt het account geblokkeerd en kan reset slechts plaatsvinden via de Servicedesk na adequate authenticatie;
4) Gebruikers kunnen op elk moment hun wachtwoord wijzigen. Bij het wijzigen van het wachtwoord moet ter controle eerst het oude wachtwoord worden ingegeven;
5) De gebruiker wordt 5.1.2.i dagen na laatste wijziging gedwongen zijn/haar wachtwoord/wachtzin te wijzigen. De gebruiker wordt 5.1.2.i dagen voor het verlopen van de geldigheid van zijn/haar wachtwoord/wachtzin hiervan in kennis gesteld;

6) Indien de gebruiker niet beschikt over het oude wachtwoord/wachtzin, dient voorafgaand aan een reset van het wachtwoord/wachtzin, via andere middelen de authenticiteit van de aanvrager voldoende gewaarborgd te worden;
7) Hergebruik van eerder gebruikte wachtwoorden/wachtzinnen is pas na 5.1.2.i wachtwoordwijzigingen toegestaan;
8) Gebruikers kunnen hun wachtwoord/wachtzin 5.1.2.i per dag zelf wijzigen;
9) Een tijdelijk wachtwoord (zoals bijvoorbeeld uitgegeven door beheer, Servicedesk of via SMS) wordt tijdens de eerstvolgende inlogsessie van de gebruiker door de laatste gewijzigd;
10) Een tijdelijk wachtwoord is 5.1.2.i ;
11) Niet-tijdelijke wachtwoorden/wachtzinnen worden alleen versleuteld verzonden;
12) Wachtwoorden/wachtzinnen worden alleen versleuteld en niet-decodeerbaar opgeslagen.

4.2.2. Functionele accounts

Functionele accounts dienen zoveel mogelijk te worden vermeden maar kennen dezelfde wachtwoordeisen als een gewoon gebruikersaccount. De rechten van een dergelijk account moeten zo veel mogelijk worden beperkt tot het noodzakelijke.

1 – Privileged (admin of beheer) accounts

Beveiligingseisen ten aanzien van het account:

1) Een privileged (admin of beheer) account wordt aangemaakt conform de naamgevingconventie zodat de functie en gerelateerde dienst/applicatie herleidbaar is;
2) Het account is herleidbaar naar een natuurlijk persoon; er wordt een eigenaar gekoppeld;
3) Het account zelf wordt zodanig ingeregeld dat mogelijk misbruik wordt geminimaliseerd;
4) Authenticatie van een privileged account vindt altijd plaats via 5.1.2.i .

Beveiligingseisen ten aanzien van het wachtwoord/wachtzin:

1) Elk privileged (admin of beheer) account heeft een uniek wachtwoord/wachtzin;
2) Het wachtwoord/wachtzin is 5.1.2.i lang, alfanumeriek met vreemde tekens;
3) Wachtwoord/wachtzin mag niet gelijk zijn aan 24 voorgaande wachtwoorden;
4) Wachtwoorden worden niet opgeschreven (of op een andere wijze onbeveiligd opgeslagen);
5) Een wachtwoord/wachtzin wordt onmiddellijk gewijzigd indien het vermoeden bestaat dat het bekend is geworden aan een derde;
6) Het wachtwoord/wachtzin moet minimaal 5.1.2.i worden gewijzigd;
7) Beheerders kunnen het wachtwoord/wachtzin 5.1.2.i per dag zelf wijzigen;
8) Na het 5.1.2.i ingeven van een foutief wachtwoord/wachtzin, wordt de toegang geblokkeerd.

2 – Service accounts

Beveiligingseisen ten aanzien van het account:

1) Het account is herleidbaar naar een natuurlijk persoon; er wordt een eigenaar gekoppeld;
2) Het account wordt aangemaakt conform de naamgevingconventie zodat de functie en gerelateerde dienst/applicatie herleidbaar is;
3) Het account zelf wordt zodanig ingeregeld dat mogelijk misbruik wordt geminimaliseerd.
4) Elk service account heeft een uniek wachtwoord/wachtzin;
5) Policy User Rights Assignment:
    a. 5.1.2.i
    b. 5.1.2.i

Beveiligingseisen ten aanzien van het wachtwoord/wachtzin:

1) Het wachtwoord/wachtzin wordt via een procedure door het systeem gegenereerd en eenmalig vastgelegd in de AD[3];
2) Het wachtwoord/wachtzin is 5.1.2.i lang, alfanumeriek met vreemde tekens[4];
3) Wachtwoorden/wachtzinnen worden niet opgeschreven (of op een andere wijze onbeveiligd opgeslagen);
4) Een wachtwoord/wachtzin wordt onmiddellijk gewijzigd indien het vermoeden bestaat dat het bekend is geworden aan een onbevoegde;

[3] Voor Linux systemen wordt dit vastgelegd 5.1.2.i

[4] De beleidsregel 5.1.2.i voor, na risicoanalyse en op verzoek van Sector IB is dit aangescherpt

5. Verantwoordelijkheden

Iedere applicatie eigenaar is verantwoordelijk voor het 5.1.2.i maken van zijn of haar applicatie en het accepteren van deze eisen. De juiste inrichting op dit vlak van de 5.1.2.i ligt bij de Product Owner van IAM (Identity and Access Management). De leidinggevenden van de personen met deze rol zullen met regelmaat moeten nagaan of dit naar behoren wordt uitgevoerd.

6. Gerelateerde beleidsdocumenten

- Privileged Authenticatie Management beleid (PAM beleid)
- Identity & Access Management beleid (IAM beleid)

7. Afwijkingen

Afwijken van deze beveiligingseisen kan alleen nadat via de Sector Informatie Beveiliging een risicoanalyse heeft plaatsgevonden en goedkeuring is verleend door de CISO. Iedere afwijking wordt gedocumenteerd.

8. Gehanteerde brondocumenten

Versie	Datum	Omschrijving	Verwijzing
5.1.2.i			
5.1.2.i			
5.1.2.i			
5.1.2.i			
1.0	Jan. 2020	Vorige versie wachtwoordbeleid	Zal verwijderd worden

Tabel 1 - Gehanteerde brondocumenten