Informatieclassificatie Vlaamse overheid (Vo-ICR)

Privileged Access Management (PAM)

Minimale maatregelen

Team Informatieveiligheid| Digitaal Vlaanderen

AGENTSCHAP
DIGITAAL VLAANDEREN
HAVENLAAN 88 BUS 60, 1000 BRUSSEL

Dit is een document voor publiek gebruik

INHOUD VAN DIT DOCUMENT

Situering van het document

Dit document maakt deel uit van de begeleidende documentatie in context van het generieke informatieclassificatieraamwerk (ICR) van de Vlaamse overheid (Vo) op initiatief van het Stuurorgaan Vlaams Informatie- en ICT Beleid.

Doel van het document

Dit document beschrijft de kwaliteitseisen van de minimale maatregelen die moeten afgedwongen worden in het kader van de deelprocessen Priviliged Access Management (PAM). Deze kwaliteitseisen worden verbonden aan de informatieklassen zoals deze zijn beschreven in het ICR van de Vo.

Werkprincipe van het document

Het huidige document bestaat uit 3 delen. Eerst worden de minimale maatregelen besproken, alvorens in het 2de deel al de nodige aanvullende informatie ter beschikking wordt gesteld, vervolgens bespreken we de link met andere maatregelen.

De organisatie van de maatregelen in het kader van informatieclassificatie wordt beschreven in het document 'Vo informatieclassificatie – Organisatie - Informatieclassificatieraamwerk'.

Verspreiding van het document

Dit document is voornamelijk voor intern gebruik en bevat informatie die mag gedeeld worden met personen verbonden aan de Vo en zijn diensten leveranciers.

Het document mag gedeeld worden met derden onder de richtlijnen openbaarheid van bestuur van de Vlaamse regering.

Vrijwaring

Dit document geeft de huidige status en daaraan gerelateerde informatie binnen het project weer. Gelieve de auteur of de bevoegde project begeleiders te contacteren om zich ervan te vergewissen dat u de laatst gevalideerde versie van dit document in handen heeft.

Eigenaar

Voorzitter werkgroep informatieveiligheid | Digitaal Vlaanderen

security@vlaanderen.be

Classificatie

Dit document valt onder de vertrouwelijkheidsklasse 1 (Publiek) en mag toegankelijk zijn voor iedereen.

Dit document valt onder integriteitsklasse 2. De organisatie heeft **geen directe hinder** indien de informatie gewijzigd wordt door onbevoegden en de **dienstverlening blijft gegarandeerd**. Maar bijsturing van de criteria en/of maatregelen is aangewezen.

Historiek

	Datum	Auteur	Opmerkingen
v.0.1	14 februari 2018	Johan SMEKENS	Eerste draft
v.0.2	21 februari 2018	Johan SMEKENS	Project review
v.0.3	9 maart 2018	Johan SMEKENS	Eerste publieke review
v.0.4	12 maart 2018	Johan SMEKENS	Verwerking opmerkingen
v.1.0	29 augustus 2018	Johan SMEKENS	〉 Aanpassingen referenties externe documenten 〉 Verwerking opmerkingen 〉 Publicatie
v.1.1	29 september 2020	Beau JANSSEN	〉 Introductie van kwaliteitskenmerk Integriteit en aanverwante controles 〉 Tekstuele aanpassingen
v.1.2	14 oktober 2020	Beau JANSSEN	Aanpassingen na de Taakgroep Integriteit
v.1.3	28 september 2021	Beau JANSSEN	Toevoegen criterium Beschikbaarheid
v.2.0	22 juli 2022	Kristel VAN AKEN	Verbeteren leesbaarheid Geen inhoudelijke wijzigingen
V.2.1	17 oktober 2023	Nele Lowet	Update KSZ

Bronnen en verwijzingen

De inhoud van dit document werd samengesteld op basis van volgende documenten:

Documentverwijzingen:

- Vo Informatieclassificatie – Organisatie Informatieveiligheid (PDF)
- Vo Informatieclassificatie – Organisatie Informatieclassificatieraamwerk (PDF)
- Vo Informatieclassificatie – Minimale maatregelen – (PDF):
  - Vo Informatieclassificatie - Minimale maatregelen – wijzigingsbeheer
  - Vo Informatieclassificatie - Minimale maatregelen – IAM
  - Vo Informatieclassificatie - Minimale maatregelen – asset en configuratiebeheer
  - Vo Informatieclassificatie - Minimale maatregelen – SIEM
  - Vo Informatieclassificatie - Minimale maatregelen – risicoanalyse
  - Vo Informatieclassificatie - Minimale maatregelen – proces risicobeheer
  - Vo Informatieclassificatie - Beleidsdocument – Risico Methodiek 1.0
- Vo Informatieclassificatie – Overzicht baseline maatregelen (XLS)

De laatste versies van deze documenten zijn te raadplegen op vlaanderen.be.

Inhoudsopgave

INHOUD VAN DIT DOCUMENT 2
Situering van het document 2
Doel van het document 2
Werkprincipe van het document 2
Verspreiding van het document 2
Vrijwaring 2
Eigenaar 2
Classificatie 3
Historiek 3
Bronnen en verwijzingen 3
INLEIDING 5
1. MINIMALE MAATREGELEN 6
1.1 Minimale algemene maatregelen 6
1.2 Minimale specifieke (GDPR) maatregelen 14
1.3 Minimale specifieke (NISII) maatregelen 15
1.4 Minimale specifieke (KSZ) maatregelen 15
2. AANVULLENDE INFORMATIE OVER DE MAATREGELEN 16
2.1. Gebruik van de maatregelen in operationele context 16
2.2. Rapportering in functie PAM 18
3. LINK MET ANDERE MAATREGELEN 19
3.1. Link met andere Beleidsdocumenten 19
3.1.1. Wijzigingsbeheer als maatregel 19
3.1.2. Identity & Access Management als maatregel 19
3.1.3. Configuratiebeheer als maatregel 20
3.1.4. Veiligheidslogging en monitoring als maatregel 21
3.1.5. Risicobeheer als maatregel 22
3.2. Een overzicht van de interacties tussen de maatregelen 22
3.2.1. Operationeel beheer 22
3.2.2. Toegangsbeheer 23
3.2.3. Logbeheer 24
3.2.4. Risicorapportering 24
3.2.5. Het proces 25

INLEIDING

De maatregel PAM of Privileged Access Management is een strikte toepassing en opvolging van een aantal basisprocessen die er in het kort om gaan om de handelingen van een profiel met beheerdersrechten:

- Te beperken tot de noodzakelijke handelingen
- Te loggen
- Te verifiëren
- Auditeerbaar te maken

Het objectief van PAM is om ervoor te zorgen dat een Beheerder van een asset zijn geprivilegieerde toegang enkel kan gebruiken voor de bedoelde intentie. De asset waartoe de Beheerder toegang wil, noemen we hier de target.

Om dit te kunnen bewerkstelligen, is er een direct verband met verschillende Beleidsdocumenten en (IT-)processen. Meer bepaald is er een link met:

- Het beheer van wijzigingen (Change management)
- Het beheer van configuraties (Configuration management)
- Het configuratiebeheer bevat naast de informatieverwerking configuratie ook alle details over de toegangsmogelijkheden tot de informatieverwerking

Opmerking: We beschouwen het beheer van opeenvolgende configuratie versies of 'Release management' binnen dit document niet als apart proces maar als een interactie tussen configuration management en change management

- Identiteits- en toegangsbeheer of Identity & Access Management (IAM)
- Log beheer (Log management)
- Risicobeheer op basis van:
  - Rapportering van operationele risico's
  - Informatie uit bovenstaande processen of operationeel riskmanagement (ORM)

Dit document legt uit hoe deze processen interageren met het Privileged Access Management-principe. Tezelfdertijd leggen we de verschillende niveaus uit die we binnen PAM erkennen en hoe deze de veiligheid van bedrijfsinformatie borgen.

Deze niveaus zijn gebaseerd op de veiligheidsbouwsteen PAMaaS, die een 1-op-1 implementatie is van dit Beleidsdocument. Ook zonder afname van deze veiligheidsbouwsteen zijn dit de logische verschillende niveaus binnen dit proces en zijn verhouding tot de Klasses van het ICR.

1. MINIMALE MAATREGELEN

1.1 Minimale algemene maatregelen

Vertrouwelijkheid

IC klasse	Minimale maatregelen
 	Klasse 1 en Klasse 2 kennen dezelfde maatregelen: 〉 IAM: 〉〉 Sterke identificatie via de federale overheid of afgeleide gecertifieerde bron (CSAM, Itsme,…) 〉〉 Authenticatie maatregelen: EID.AS (Substantial) 〉〉 Autorisatie: Autorisatie registratie via toegangsbeheerproces 〉〉 Autorisatie validatie: 〉〉〉 Onderwerp mag niet deelnemen aan de validatie van de betrokken autorisatie (SoD / toegangsautorisatie) 〉〉〉 Jaarlijkse periodieke herziening van de toegangen: 〉〉〉 Hervalidatie toegang mogelijk op basis van eenvoudige motivatie; 〉〉〉 Maximale duurtijd van de toegangsautorisatie in theorie onbeperkt, maar verplicht af te stemmen met reële noodzaak tot toegang (least access). 〉 Configuration Management: 〉〉 Generieke documentatie van de toegangen, accounts, rollen: technisch noodzakelijke toegangen op basis van het least access principe 〉〉 Generieke documentatie access controle baseline voor de betrokken informatieverwerkingscomponenten: 〉〉〉 Rollen in relatie least access principe 〉〉〉 Communicatieprotocol beschrijving 〉〉〉 Authenticatie protocol beschrijving 〉〉〉 Configuration and data protection (Network en malware bedreigingen) 〉 Log informatie: 〉〉 Toegang logs 〉〉 (Lokaal) Toegangsbeheer log info (OS, Middleware, applicatie) 〉〉 Privilege elevation log 〉〉 Memory dump log 〉〉 Log configuratie log 〉〉 Log informatie op de infrastructuur ter beschikking houden gedurende 3 maand 〉 Reporting: Operationele opvolging toegangsbeheer op de gehele informatieverwerking ketting (inclusief werkstations) 〉 Jaarlijkse review privileged toegangen (toegangsbeheer) 〉 Operationeel risicobeheer toegangsconfiguratie (Minimaal om de 12 maanden):

	〉 Identificatie en verwijderen van privileged accounts 〉 Slapende accounts (Laatst gebruikt > 1 jaar) 〉 Disabled accounts (Laatst gebruikt > 3 maand) 〉 Orphan accounts 〉 Orphan (wees) accounts zijn accounts zonder relatie met een fysieke identiteiten: 〉 Accounts zonder geïdentificeerde eigenaar 〉 Relatie met een toepassing zonder toepassingsverantwoordelijke 〉 Paswoord policy opvolging interactieve accounts 〉 Paswoorden ouder dan 3 maand
	Alle maatregelen van Klasse 1 / Klasse 2 + 〉 IAM: 〉 Authenticatie: Er is geen permanente toegang tot de authenticatie middelen 〉 Autorisatie: 〉 Validatie met goedkeuring van een door de organisatie geautoriseerd tweede persoon (SoD/4EYES op niveau toegangsautorisatie) 〉 Voorbeeld: Lokale beheerder doet de registratie en deze wordt gevalideerd door de leidinggevende van het onderwerp of de toepassingsbeheerder 〉 Jaarlijkse periodieke herziening van de toegangen 〉 Revalidatie toegang mogelijk op basis van motivatie door hiërarchische of toepassing verantwoordelijke 〉 Change Management: 〉 Registratie van de motivatie tot toegang door middel van volgende change specificaties zijn toegestaan: 〉 Change duurtijd is gebaseerd op functionele noodzaak 〉 Pre-approved changes zijn toegestaan. Reguliere operationele opvolgingstaken door de informatieverwerker hebben een maximale duurtijd van 1 jaar. Ook hier kijkt men erop toe dat de toegangen beperkt zijn tot het absolute noodzakelijke. 〉 Standaard changes in context van geplande aanpassingen of preventieve instandhouding van de informatieverwerking. 〉 Dringende (emergency) changes op basis van een geregistreerd incident met de bedoeling de beschikbaarheid van de informatieverwerking te garanderen. 〉 Post-mortem validatie van de validatie (Anomalie rapportering) 〉 Configuration Management: 〉 Generieke documentatie van de toegangen, accounts, rollen, protocolgebruik 〉 Auditeerbaarheid van de configuratie garanderen 〉 Operationeel risicobeheer naar kwetsbaarheden

	〉 Operationeel risicobeheer naar proces efficiëntie: inactieve en slapende accounts (uitgezonderd systeem accounts) 〉 Log informatie: 〉 Change log in context Log correlatie 〉 Op de infrastructuur ter beschikking houden gedurende 1 maand 〉 Log historiek verwerken via een log management systeem (SYSLOG) 〉 Log correlatie in context PAM 〉 Log historiek offline archiveren gedurende 1 jaar 〉 Session recording (4EYES) beschikbaar houden gedurende 1 jaar 〉 Log Management: 〉 Afgedwongen log configuratie met gegarandeerd resultaat 〉 Afgedwongen log centralisatie met gegarandeerd resultaat 〉 Reporting: Operationele opvolging privileged toegangen 〉 Opvolging motivatie tot toegang tot informatieverwerking infrastructuur, middleware en toepassingscomponenten 〉 Opvolging toegangsconfiguratie / opsporen 'achterdeuren'
	Alle maatregelen van Klasse 1 / Klasse 2 + + Klasse 3 〉 IAM: 〉 Authenticatie: 〉 Er is geen permanente toegang tot de authenticatie middelen 〉 Motivatie tot gebruik van de toegang wordt gevalideerd door de informatieverwerker (4EYES op motivatie gebruik toegang) 〉 Autorisatie: 〉 Validatie met goedkeuring van een door de organisatie geautoriseerd tweede en derde persoon (SoD/4EYES op niveau toegangsautorisatie) 〉 Voorbeeld: Lokale beheerder doet de registratie en deze wordt gevalideerd door de leidinggevende van het onderwerp én de toepassingsbeheerder 〉 Periodieke herziening van de toegangen, langer dan 1 jaar zijn niet toegestaan. Nieuw toegangsverzoek noodzakelijk. 〉 Change Management: 〉 Change duurtijd is altijd gebaseerd op functionele noodzaak 〉 De functionele noodzaak is steeds gedocumenteerd in de change. 〉 Onderstaande types van changes zijn toegestaan: 〉 Standaard changes in context van geplande aanpassingen of preventieve instandhouding van de informatieverwerking. 〉 Dringende (emergency) changes op basis van een geregistreerd incident met de bedoeling de beschikbaarheid van de informatieverwerking te garanderen. 〉 Pre-approved changes (voor o.a. reguliere operationele opvolgingstaken door de informatieverwerker) zijn niet toegestaan (Enkel geautomatiseerde opvolging onder strikte configuratie controle)

	〉 4EYES validatie van het gebruik van de toegang door operationeel verantwoordelijke op basis van aangeleverde change validatie 〉 4EYES opvolging van de activiteiten 〉 Log informatie: 〉 Log historiek offline archiveren gedurende 3 jaar 〉 Session recording (4EYES) beschikbaar houden gedurende 1 jaar
	Alle maatregelen van Klasse 1 / Klasse 2 + Klasse 3 + Klasse 4 + 〉 IAM: 〉 Authenticatie: 〉 EID.AS (High) 〉 EID.AS (Substancial toegestaan bij technische beperkingen) 〉 Autorisatie: 〉 Duurtijd van een toegangsverzoek beperkt tot functionele noodzaak. 〉 Periodieke herziening van de toegangen niet toegestaan. Nieuw toegangsverzoek noodzakelijk.

Integriteit

IC klasse	Minimale maatregelen
 	Klasse 1 en Klasse 2 kennen dezelfde maatregelen: 〉 IAM: 〉 Sterke identificatie via de federale overheid of afgeleide gecertifieerde bron (CSAM, Itsme,…) 〉 Authenticatie maatregelen: EID.AS (Substantial) 〉 Autorisatie: Autorisatie registratie via toegangsbeheerproces 〉 Autorisatie validatie: 〉 Onderwerp mag niet deelnemen aan de validatie van de betrokken autorisatie (SoD / toegangsautorisatie) 〉 Jaarlijkse periodieke herziening van de toegangen: 〉 Hervalidatie toegang mogelijk op basis van eenvoudige motivatie; 〉 Maximale duurtijd van de toegangsautorisatie in theorie onbeperkt, maar verplicht af te stemmen met reële noodzaak tot toegang (least access). 〉 Configuration Management: 〉 Generieke documentatie van de toegangen, accounts, rollen: technisch noodzakelijke toegangen op basis van het least access principe 〉 Generieke documentatie access controle baseline voor de betrokken informatieverwerkingscomponenten:

	〉 Rollen in relatie least access principe 〉 Communicatieprotocol beschrijving 〉 Authenticatie protocol beschrijving 〉 Configuration and data protection (Network en malware bedreigingen) 〉 Log informatie: 〉 Toegang logs 〉 (Lokaal) Toegangsbeheer log info (OS, Middleware, applicatie) 〉 Privilege elevation log 〉 Memory dump log 〉 Log configuratie log 〉 Log informatie op de infrastructuur ter beschikking houden gedurende 3 maand 〉 Reporting: Operationele opvolging toegangsbeheer op de gehele informatieverwerking ketting (inclusief werkstations) 〉 Jaarlijkse review privileged toegangen (toegangsbeheer) 〉 Operationeel risicobeheer toegangsconfiguratie (Minimaal om de 12 maanden): 〉 Identificatie en verwijderen van privileged accounts 〉 Slapende accounts (Laatst gebruikt > 1 jaar) 〉 Disabled accounts (Laatst gebruikt > 3 maand) 〉 Orphan accounts 〉 Orphan (wees) accounts zijn accounts zonder relatie met een fysieke identiteiten: 〉 Accounts zonder geïdentificeerde eigenaar 〉 Relatie met een toepassing zonder toepassingsverantwoordelijke 〉 Paswoord policy opvolging interactieve accounts 〉 Paswoorden ouder dan 3 maand
	Alle maatregelen van Klasse 1 / Klasse 2 + 〉 IAM: 〉 Authenticatie: Er is geen permanente toegang tot de authenticatie middelen 〉 Autorisatie: 〉 Validatie met goedkeuring van een door de organisatie geautoriseerd tweede persoon (SoD/4EYES op niveau toegangsautorisatie) 〉 Voorbeeld: Lokale beheerder doet de registratie en deze wordt gevalideerd door de leidinggevende van het onderwerp of de toepassingsbeheerder 〉 Jaarlijkse periodieke herziening van de toegangen 〉 Revalidatie toegang mogelijk op basis van motivatie door hiërarchische of toepassing verantwoordelijke 〉 Change Management:

	〉 Registratie van de motivatie tot toegang door middel van volgende change specificaties zijn toegestaan: 〉 Change duurtijd is gebaseerd op functionele noodzaak 〉 Pre-approved changes zijn toegestaan. Reguliere operationele opvolgingstaken door de informatieverwerker hebben een maximale duurtijd van 1 jaar. Ook hier kijkt men erop toe dat de toegangen beperkt zijn tot het absolute noodzakelijke. 〉 Standaard changes in context van geplande aanpassingen of preventieve instandhouding van de informatieverwerking. 〉 Dringende (emergency) changes op basis van een geregistreerd incident met de bedoeling de beschikbaarheid van de informatieverwerking te garanderen. 〉 Post-mortem validatie van de validatie (Anomalie rapportering) 〉 Configuration Management: 〉 Generieke documentatie van de toegangen, accounts, rollen, protocolgebruik 〉 Auditeerbaarheid van de configuratie garanderen 〉 Operationeel risicobeheer naar kwetsbaarheden 〉 Operationeel risicobeheer naar proces efficiëntie: inactieve en slapende accounts (uitgezonderd systeem accounts) 〉 Log informatie: 〉 Change log in context Log correlatie 〉 Op de infrastructuur ter beschikking houden gedurende 1 maand 〉 Log historiek verwerken via een log management systeem (SYSLOG) 〉 Log correlatie in context PAM 〉 Log historiek offline archiveren gedurende 1 jaar 〉 Session recording (4EYES) beschikbaar houden gedurende 1 jaar 〉 Log Management: 〉 Afgedwongen log configuratie met gegarandeerd resultaat 〉 Afgedwongen log centralisatie met gegarandeerd resultaat 〉 Reporting: Operationele opvolging privileged toegangen 〉 Opvolging motivatie tot toegang tot informatieverwerking infrastructuur, middleware en toepassingscomponenten 〉 Opvolging toegangsconfiguratie / opsporen ‘achterdeuren’

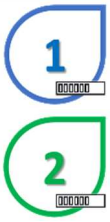
<table>
<tr>
<td>  </td>
<td>Alle maatregelen van Klasse 1 / Klasse 2 + + Klasse 3

〉 IAM:
〉 Authenticatie:
〉 Er is geen permanente toegang tot de authenticatie middelen
〉 Motivatie tot gebruik van de toegang wordt gevalideerd door de informatieverwerker (4EYES op motivatie gebruik toegang)
〉 Autorisatie:
〉 Validatie met goedkeuring van een door de organisatie geautoriseerd tweede en derde persoon (SoD/4EYES op niveau toegangsautorisatie)
〉 Voorbeeld: Lokale beheerder doet de registratie en deze wordt gevalideerd door de leidinggevende van het onderwerp én de toepassingsbeheerder
〉 Periodieke herziening van de toegangen, langer dan 1 jaar zijn niet toegestaan. Nieuw toegangsverzoek noodzakelijk.
〉 Change Management:
〉 Change duurtijd is altijd gebaseerd op functionele noodzaak
〉 De functionele noodzaak is steeds gedocumenteerd in de change.
〉 Onderstaande types van changes zijn toegestaan:
〉 Standaard changes in context van geplande aanpassingen of preventieve instandhouding van de informatieverwerking.
〉 Dringende (emergency) changes op basis van een geregistreerd incident met de bedoeling de beschikbaarheid van de informatieverwerking te garanderen.
〉 Pre-approved changes (voor o.a. reguliere operationele opvolgingstaken door de informatieverwerker) zijn niet toegestaan (Enkel geautomatiseerde opvolging onder strikte configuratie controle)
〉 4EYES validatie van het gebruik van de toegang door operationeel verantwoordelijke op basis van aangeleverde change validatie
〉 4EYES opvolging van de activiteiten
〉 Log informatie:
〉 Log historiek offline archiveren gedurende 3 jaar
〉 Session recording (4EYES) beschikbaar houden gedurende 1 jaar</td>
</tr>
<tr>
<td>  </td>
<td>Alle maatregelen van Klasse 1 / Klasse 2 + Klasse 3 + Klasse 4 +

〉 IAM:
〉 Authenticatie:
〉 EID.AS (High)
〉 EID.AS (Substancial toegestaan bij technische beperkingen)
〉 Autorisatie:
〉 Duurtijd van een toegangsverzoek beperkt tot functionele noodzaak.</td>
</tr>
</table>

	〉 Periodieke herziening van de toegangen niet toegestaan. Nieuw toegangsverzoek noodzakelijk.

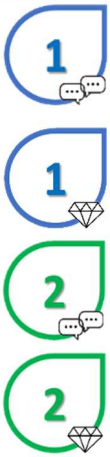
Beschikbaarheid

IC klasse	Minimale maatregelen
	Klasse 1 en Klasse 2 kennen dezelfde maatregelen: 〉 Beschikbaarheid van het proces is minimaal kantooruren (5d x 10u)
	Klasse 3 en Klasse 4 en Klasse 5 kennen dezelfde maatregelen: 〉 Beschikbaarheid van het proces is 24u x 7d

1.2 Minimale specifieke (GDPR) maatregelen

De minimale algemene maatregelen voor PAM moeten toegepast worden: per klasse zijn de overeenkomende maatregelen van toepassing (zie hoofdstuk 'minimale algemene maatregelen').

Vertrouwelijkheid en integriteit

IC klasse	Minimale maatregelen
	Er zijn geen GDPR specifieke maatregelen voor klasse 1 en Klasse 2.
	Klasse 3 en klasse 4 kennen dezelfde maatregelen: 〉 Gedetailleerde logging op applicatieniveau van **alle toegangen tot de informatie** 〉 Inkijken van detailinformatie 〉 Aanpassingen aan detailinformatie 〉 Verwijderen van detailinformatie
	Er zijn geen GDPR maatregelen voor klasse 5.

Beschikbaarheid

Er zijn geen GDPR specifieke maatregelen gedefinieerd in het kader van beschikbaarheid.

1.3 Minimale specifieke (NISII) maatregelen

In afwachting van de goedkeuringen omtrent NISII is er in dit document alvast de nodige ruimte voorzien voor toekomstige minimale specifieke NISII maatregelen.

1.4 Minimale specifieke (KSZ) maatregelen

Volgens de Minimale Normen van de Kruispuntbank Sociale Zekerheid moeten volgende maatregelen in het kader van PAM toegepast worden:

Beschikbaarheid, Integriteit & Vertrouwelijkheid

IC klasse	Minimale maatregelen
	Klasse 1 t/m Klasse 5 kennen dezelfde maatregelen: 〉 Elke organisatie moet de toegang van informatiebeheerders tot informaticasystemen beperken door identificatie, authenticatie, en autorisatie (Ref. KSZ 5.6.5). 〉 Voorkomen dat een enkele persoon alleen de controle zou verwerven over dit proces (in productie stelling) (Ref. KSZ 5.9.2).

2. AANVULLENDE INFORMATIE OVER DE MAATREGELEN

2.1. Gebruik van de maatregelen in operationele context

We onderscheiden drie implementatieniveaus van de minimale maatregel PAM. Elk van deze niveaus laat de gebruiker toe om zowel de functionele behoeften bij de beheersactiviteiten in te vullen én tegemoet te komen aan de informatieverwerkingseisen die we terugvinden in de implementatiecriteria.

- Het **laagste** niveau van implementatie van de PAM maatregel bevat:
- Toegangsbeheer
- Sterke identificatie van de gebruiker van het PAM-proces
- Dit is een minimale voorwaarde om toegang te verlenen tot het PAM-proces
- Sterke authenticatie laat toe om de identiteit achter alle operationele activiteiten te controleren
- Elke toegang is geautoriseerd door de toegangsbeheerder en minstens jaarlijks valideert de toepassingseigenaar de toegangsrechten
  Er is een permanente, gemonitorde toegang tot het target account waarmee de privileged toegangen worden verworven
- Change, configuratie en release management
- Motivatie van de gebruiker om toegang te krijgen tot het target is niet verplicht
  Er is geen verplichte integratie van change managementinformatie
- Auditeerbaarheid is gebaseerd op documentatie en punctuele ad hoc audits van zowel de operationele processen als de informatie verwerkende configuraties (Basis ISO27001/-2 dekt de generieke verwerkingscontext af)
- Toepassingsgebied
- Dit toepassingsniveau is geschikt voor beheer van componenten die algemene informatie verwerk tot en met **[Informatieklasse 3]** en dit voor zowel Vertrouwelijkheid als Integriteit.
- Dit toepassingsniveau is **niet geschikt** voor de verwerking van persoonsgegevens

In dit niveau kan, bij niet-afname van de bouwsteen PAMaaS, het PAM-proces volledig manueel verlopen.

- Het **middelste** niveau van implementatie van de PAM maatregel bevat:
- Toegangsbeheer
- Sterke identificatie van de gebruiker van het PAM-proces
- Dit is een minimale voorwaarde om toegang te verlenen tot het PAM-proces
- Sterke authenticatie laat toe om de identiteit achter alle operationele activiteiten te controleren
- Elke toegang is geautoriseerd door de toegangsbeheerder en minstens jaarlijks valideert de toepassingseigenaar de toegangsrechten
  Er is een permanente gemonitorde en **gemotiveerde** toegang tot het target account waarmee de privileged toegangen worden verworven
  Alle activiteiten tijdens de uitvoering van de privileged toegang worden geregistreerd
  Session recording, ook manueel, maakt dat de activiteiten in real-time en uitgesteld kunnen bekeken worden.
- Change, configuratie en release management
- Er gebeurt een **verplichte validatie** van de **motivatie** van de gebruiker.

〉 Er is geen dubbele controle van de toegang op voorhand noodzakelijk. Periodieke controle gebeurt 'post-mortem' op basis van correlatie van logs die voortkomen uit de processen Change en Release Management en de logs van PAM zelf

Als je de veiligheidsbouwsteen PAMaaS afneemt, is dit een standaard rapportage.

〉 Auditeerbaarheid is gebaseerd op volgende risico rapportering
  〉 Procescontrole: werd elke toegang correct afgedekt door een geregistreerde activiteit (change)
  〉 Pre-approved changes en operationele activiteiten (Changes) met een maximale duurtijd tot één jaar zijn toegestaan voor operationele teams
〉 Periodieke risico rapportering dekt zowel de operationele processen als de informatie verwerkende configuratie
  〉 Alle activiteiten van de gebruiker van het PAM-proces worden geregistreerd. Dit is de implementatie van het controleprincipe op basis van manueel logboek registratie of geautomatiseerde session recording in combinatie met de log informatie
〉 Toepassingsgebied
〉 Dit toepassingsniveau is geschikt voor beheer van componenten die algemene informatie verwerk tot en met **[Informatieklasse 4]** en dit voor zowel Vertrouwelijkheid als Integriteit.
〉 Dit toepassingsniveau **is geschikt** bij de verwerking van persoonsgegevens tot en met **[Informatieklasse 3]** en dit enkel voor Vertrouwelijkheid

In dit niveau is een automatische invulling van PAM verplicht. Het afnemen van PAMaaS is echter niet verplicht – entiteiten kunnen dit ook zelf invullen.

〉 Het **hoogste** niveau van implementatie van de PAM maatregel bevat:
〉 Toegangsbeheer
〉 Sterke identificatie van de gebruiker van het PAM-proces
〉 Dit is een minimale voorwaarde om toegang te verlenen tot het PAM-proces
〉 Sterke authenticatie laat toe om de identiteit achter alle operationele activiteiten te controleren
〉 Elke toegang is geautoriseerd via toegangsbeheer op basis van functionele noodzaak. Denk hierbij aan een interventie in kader van een incident.
  Er is geen permanente toegang tot het account met privileged toegangen binnen de informatieverwerking
  Er is een permanente gemonitorde en **gemotiveerde** toegang tot het target account waarmee de privileged toegangen worden verworven
  Alle activiteiten tijdens de uitvoering van de privileged toegang worden geregistreerd
  Session recording, ook manueel, maakt dat de activiteiten in realtime en uitgesteld kunnen bekeken worden.
〉 Change, configuratie en release management
〉 Er gebeurt een verplichte validatie van de motivatie van de gebruiker.
〉 Er is een dubbele controle voorzien op de aangeleverde motivatie vooraleer toestemming kan gegeven worden voor de toegang.
〉 De periodieke controle gebeurt net als bij de medium implementatie van het PAM-proces 'post-mortem' op basis van logs die voortkomen uit de processen Change en Release Management en de logs van PAM zelf
〉 Auditeerbaarheid is gebaseerd op volgende risico rapportering
  Procescontrole: werd elke toegang correct afgedekt door een geregistreerde activiteit (change)

Pre-approved changes en operationele activiteiten (Changes) zijn beperkt tot de reële functionele duurtijd van de activiteiten

- Periodieke risicorapportering dekt zowel de operationele processen als de informatie verwerkende configuratie
- Alle activiteiten van de gebruiker van het PAM-proces worden geregistreerd.
  Dit is de implementatie van het 4EYES principe op basis van manueel logboek registratie of geautomatiseerde session recording in combinatie met de log informatie
- Toepassingsgebied
- Dit toepassingsniveau is geschikt voor beheer van **alle** componenten in de informatie verwerken, en dit dus vanzelfsprekend voor zowel Vertrouwelijkheid als Integriteit

2.2. Rapportering in functie PAM

Proces anomalieën

- Proces anomalieën worden opgespoord op basis van de correlaties van informatie uit verschillende processen of hun ondersteunende technische platformen
- Input:
  - Change log (Bron: Wijzigingsbeheer)
  - PAM log (Bron: Operationeel beheer informatieverwerking)
- Output:
  - Niet-gemotiveerde toegangen op basis van het ontbreken van een change record
  - Niet-gemotiveerde toegangen op basis van een ongeldig change record
- Toegang buiten het gevalideerde change venster (tijdframe)
- Toegang op basis van een niet gevalideerde change.
- Tijd van toestemming wordt gebruikt om antidatering te detecteren.
- Doel:
  - Operationele toegang tot informatieverwerking infrastructuur verantwoorden door gebruik te maken van de change managementprocessen
  - Niet geautoriseerde toegangen opsporen en corrigerende maatregelen initiëren

Configuratie anomalieën

- Configuratie anomalieën worden opgespoord op basis van de correlaties van informatie uit het PAM proces en de technische log uit de informatieverwerkingscomponenten
- Input:
  - PAM log (Bron: Operationeel beheer informatieverwerking)
  - Target log (Bron: Configuratie beheer van de technische component; Voorbeeld: security log host, middleware of toepassing)
- Output:
  - Identificatie van toegangen tot de informatieverwerking die buiten het PAM proces verlopen
- Doel:
  - Efficiëntie van het PAM proces aantonen door het actief opsporen van achterdeur toegangen
  - Niet geautoriseerde toegangen opsporen en corrigerende maatregelen initiëren

3. LINK MET ANDERE MAATREGELEN

3.1. Link met andere Beleidsdocumenten

3.1.1. Wijzigingsbeheer als maatregel

Dit document bevat geen beschrijving van de maatregel Wijzigingsbeheer (Change management) maar legt de focus op de afhankelijkheden die er zijn bij het uitrollen van een succesvol Privileged access management proces.

Afhankelijkheid van de maatregel

- Onderstaande items zijn beperkt tot de context van dit document en moeten worden gezien als integraal onderdeel van de informatieverwerking
- Generieke configuraties worden uitgewerkt in generieke baseline documentatie van waaruit ze als referentie configuratie kunnen worden toegepast.

Het change managementproces vult het criteria 'Motivatie' en 'Goedkeuring' in bij het Privileged access management proces.

Het proces verzamelt alle elementen van zowel de organisatorische behoeften als de technische behoeften en motiveert de noodzaak tot privileged toegang tot de technische componenten en potentieel ook toegang tot de verwerkte informatie tijdens de beheerstaken. Op basis van deze behoefte zal het proces zorgen voor de nodige validatie en toestemming ter begeleiding van deze beheersactiviteiten.

Concreet helpt dit proces ons om wie/wanneer/waarom te identificeren bij elke vraag tot een privileged toegang tot een informatieverwerking component, alsook wie/wanneer de nodige autorisatie(s)/goedkeuring(en) heeft gegeven.

3.1.2. Identity & Access Management als maatregel

Dit document bevat geen beschrijving van de maatregel Identity & Access Management maar legt de focus op de afhankelijkheden die er zijn bij het uitrollen van een succesvol Privileged access management proces.

Afhankelijkheid van de maatregel

- Onderstaande items zijn beperkt tot de context van dit document en moeten worden gezien als integraal onderdeel van de informatieverwerking
- Generieke configuraties worden uitgewerkt in generieke baseline documentatie van waaruit ze als referentie configuratie kunnen worden toegepast.

Het Identity & Access Management proces vult volgende criteria in:

- Identity management: identificeert elk fysiek persoon die deelneemt aan een PAM proces
- Access management:
- Levert de middelen aan om een authenticatie behoeften op een aan de informatieklasse aangepaste manier in te vullen.
- Vult de toegangsbeheer behoeften in (autorisatie) op een aan de informatieklasse aangepaste manier.

Opmerking: Het configureren van maatregelen op de technische component (access control) is ingevuld via het proces configuratie beheer.

Least access implementatie op basis van accounts en de daaraan gekoppelde rollen en uitgebreid met de access controles op het technische systeem en|of dataopslag componenten

3.1.3. Configuratiebeheer als maatregel

Dit document bevat geen detail beschrijving van de maatregel configuratiebeheer (Configuration management) maar legt de focus op de afhankelijkheden die er zijn bij het uitrollen van een succesvol Privileged access management proces.

- Een auditeerbaar configuratiebeheersproces is verplicht en het gebruikte proces, inclusief de uitwerking op basis van technische hulpmiddelen is gedocumenteerd vanaf informatie **[Klasse 3]** en dit voor zowel Vertrouwelijkheid als Integriteit (Auditeerbaarheid).

Afhankelijkheid van de maatregel

- Onderstaande items zijn beperkt tot de context van dit document en moeten worden gezien als integraal onderdeel van de informatieverwerking
- Generieke configuraties worden uitgewerkt in generieke baseline documentatie van waaruit ze als referentie configuratie kunnen worden toegepast.

Het configuratiebeheersproces controleert de implementatie parameters en omvat oa.

- De toegangscontroles van een correct toegangsbeheer.
  Wat zijn de functionele verwachtingen die worden ingevuld door de betrokken toegangscontroles (Least access principe is een noodzaak)
- Hoe de verschillende toegangsrollen technisch uitgewerkt
- Hoe controleren we de implementatie van deze toegangscontroles (Auditeerbaarheid van de toegangscontrole)
- Controle op de log configuratie, deze worden als basiselement in context van auditeerbaarheid van de operationele informatieverwerking gebruikt
- Wat zijn de functionele verwachtingen die worden ingevuld door de betrokken log configuratie
- Hoe is deze configuratie technisch uitgewerkt
- Operationele opvolging op basis van rapporten
- Operationele opvolging op basis van alerts (real-time mogelijk)
- Welke correlatie, interpretaties van log informatie resulteren in aantoonbare controle
- Auditeerbaarheid van de log als bron voor de interne controle binnen het risico beheer.

3.1.4. Veiligheidslogging en monitoring als maatregel

Dit document bevat geen detail beschrijving van de maatregel Veiligheidslogging en monitoring ('SIEM') maar legt de focus op de afhankelijkheden die er zijn bij het uitrollen van een succesvol Privileged access management proces.

Afhankelijkheid van de maatregel

- Onderstaande items zijn beperkt tot de context van dit document en moeten worden gezien als integraal onderdeel van de informatieverwerking
- Generieke configuraties worden uitgewerkt in generieke baseline documentatie van waaruit ze als referentie configuratie kunnen worden toegepast.

Log management verzamelt bronmateriaal, zowel uit technisch als operationele bronnen. Dit bronmateriaal zal dan gebruikt worden om de nodige controlemaatregelen mogelijk te maken.

- Het laat toe om log informatie uit verschillende bronnen te combineren om inzicht te krijgen op operationele risico's (Risico beheer)
- Het laat toe om in geval van een incident bij informatieverwerking een reconstructie van de verwerkingsactiviteiten te maken
  Een auditeerbaar log managementsysteem zal ook de nodige garanties geven dat de output kan gebruikt worden als juridische bewijslast.

We maken onderscheid tussen volgende bronnen als log informatie:

- Onderstaande opsomming van maatregelen is niet beperkt tot deze voorbeelden

- Technische bronnen
- Het configuratie beheerproces garandeert de correcte log configuratie parameters.
- Log entries in bestanden of databases afkomstig uit systemen, middleware en toepassingen. (Vb. Security log Windows)
  Geautomatiseerde controle van de beheersactiviteiten (Session recording) van de beheersactiviteiten (niet-geautomatiseerde controles worden gezien als organisatorische controlemaatregelen)
  Dit omvat ook de garantie op de beschikbaarheid van deze informatie door middel van archivering of retention
- Organisatorische bronnen
- Change management: Operationele log van alle change registraties in het change management tool of proces
- Operationele opvolging van de activiteiten: Opname van alle activiteiten die binnen een beheersessie manueel worden uitgevoerd door een onafhankelijk fysieke persoon.
- Deze 'fysieke' logboeken worden conform de behoeften van een geautomatiseerd systeem, geregistreerd en gearchiveerd voor potentiële audit doeleinden.

Opmerking: Het is sterk geadviseerd om de verzameling van deze logs te automatiseren om de verwerking van de controlemaatregelen te optimaliseren (resource en kost efficiëntie).

Opmerking: Logs bewaren doe je volgens het "WORM" principe: write once, read many. Je organiseert het zo dat toepassingen logs wegschrijven in bestanden die geen enkele gebruiker (fysiek of systeem) deze nog kan aanpassen. Dit dwing je technisch af. Tegelijkertijd zorg je er wel voor dat de logs consulteerbaar zijn en dat andere toepassingen (bijvoorbeeld SIEM-oplossing) ze kunnen uitlezen.

3.1.5. Risicobeheer als maatregel

Deze maatregel is een deel van het operationeel risicobeheer verbonden aan de informatieverwerking. Rapportering en operationele opvolging van deze rapporten binnen de organisatie zijn het sleutelelement bij uitstek om aan te tonen (auditeerbaarheid bewijzen) dat er effectieve opvolging gebeurt op de activiteiten van de informatieverwerker en dat alle maatregelen die genomen werden resulteren in een correcte afdekking van de (rest)risico's.

Basis rapportering operationeel risicobeheer, gebruikt binnen PAM

- Onderstaande items zijn beperkt tot de context van dit document en moeten worden gezien als integraal onderdeel van de informatieverwerking
- Generieke configuraties worden uitgewerkt in generieke baseline documentatie van waaruit ze als referentie configuratie kunnen worden toegepast.

Onderstaand type rapportering is aanwezig in de generieke context van de informatieverwerking en worden niet specifiek hernomen in context van PAM

- Beschikbaarheid bronnen (Output van Log beheer)
- Beschikbaarheid van de noodzakelijke bronnen verzekeren, deze bronnen zijn noodzakelijk zijn om de rapportering en opvolging te garanderen
- Interpretaties van technische log informatie op basis van technische criteria
  Voorbeeld: Failed paswoord pogingen, account lockout, slapende accounts, Paswoord reset,
- Interpretaties van organisatorische log informatie op basis van organisatorische criteria.
  Voorbeeld: Workflow validatie door onbevoegden

3.2. Een overzicht van de interacties tussen de maatregelen

Deze sectie van het document beschrijft de interactie tussen de verschillende maatregelen die gecombineerd resulteren in de maatregel PAM.

3.2.1. Operationeel beheer

Het operationeel beheer van de informatieverwerkingscomponenten is aangedreven door volgende basisprocessen. Vanuit deze basis worden alle betrokken beheerstoegangen zowel technisch als operationeel gemotiveerd.

- **Configuration management** of configuratiebeheer vertaalt de functionele behoeften van de informatieverwerking in een beschrijving van de (deel)component(en) in de informatieverwerking. De configuratie documentatie beschrijft alle technische details en de motivatie voor de gekozen technische (deel)oplossingen. Het resultaat van het proces zal gebruikt worden bij zowel de implementatie van de betrokken configuratie als bij een configuratie audit.
- **Release management** of opvolging van de opeenvolgende versies van de configuratie en de bijhorende documentatie. In de meeste implementaties is dit proces versmolten in het configuratiebeheersproces. Het proces registreert de functionele motivatie van de wijzigingen en de impact op de configuratie. Conform aan het configuratiebeheer zal het resultaat van het release management proces gebruikt worden bij zowel de implementatie van de aanpassingen aan de betrokken configuratie als bij een configuratie audit.

- Het **Change management** proces of opvolging van de wijzigingen slaat de brug tussen de behoeften en controles van de organisatie en het operationeel beheer gerelateerd aan de technische informatieverwerkingscomponenten. Het proces …
- Bewaakt de afspraken in context van de informatieverwerking (Service Level Agreement)
- Communiceert de agenda, motivatie en de impact van wijzigingen aan de afnemende organisatie en de operationele diensten achter de informatieverwerking
- Bewaakt de correcte uitvoering van het configuratie en versie beheerprocessen
- Beschikbaarheid ondersteunende documentatie
- Beschikbaarheid documentatie van eigenlijke configuratie aanpassingen en eventuele test resultaten (waar van toepassing)
- Zorgt voor de nodige autorisatie en motivatie voor beheerstoegangen
- De historiek van deze activiteiten noemen we een change log. Het bevat:
  - Beschrijving van de geïmpacteerde informatieverwerkingscomponenten
  - De validatie van de operationeel afspraken met de toepassingseigenaar (Al dan niet gedelegeerde of individuele goedkeuring onder de afgesproken SLA)
  - Beschrijving van de doelstelling van de wijziging en een aanduiding waar (bij wie) de configuratie en release documenten terug te vinden zijn
  - Tijdstip (datum en tijd) van aanvraag en tijdstip van goedkeuring van de wijzigingen, evenals de identiteit van de aanvragende en geconsulteerde partij(en) en de geautoriseerde persoon die de validatie heeft gedaan en de goedkeuring heeft gegeven
  - Tijdstip (datum en tijd) van uitvoering en het toegelaten tijdsgebruik waarvoor deze change registratie geldig is, evenals de identificatie van de uitvoerende persoon of organisatie
  - Tijdstip (datum en tijd) evenals de status van uitvoering bij het afsluiten van de activiteiten gelinkt aan de change

3.2.2. Toegangsbeheer

  - De traceerbaarheid van de activiteiten binnen een toepassing is niet in scope PAM
  - Traceerbaarheid van activiteiten binnen een toepassing moet worden ingevuld door maatregelen binnen de applicatie zelf (In GDPR context verwijst men dan naar privacy logging)

- Het **toegangsbeheer** proces bestaat uit meerdere deelcomponenten.
  Het Identity and Access management proces staat in voor:
  Voorbeeld: webIDM
- De correcte identificatie van de deelnemende gebruikers (Fysieke personen) in het PAM proces
- Het aanleveren van de aangepaste authenticatiemiddelen. Deze authenticatiemiddelen bestaan uit accounts en toegangsrechten (details in het IAM-document)
- De volledige traceerbaarheid van het proces startende bij de correcte identificatie van de gebruiker (identity management), de registratie van de motivatie tot toegang (request management) en de bijhorende validaties (Workflow management)
- De volledige lifecycle van de authenticatiemiddelen op de technische componenten.
- Creatie, aanpassingen, verwijderen van de authenticatiemiddelen
- Volledige traceerbaarheid van de activiteiten bij het beheer van de authenticatiemiddelen
- De traceerbaarheid van het gebruik van de authenticatiemiddelen is beschikbaar in operationele context van het betrokken technische component
- Authenticatie staat in voor:

Voorbeeld: ACM, CSAM, …

- Validatie van de gebruiker op basis van de gebruikte authenticatiemiddelen (Account)
- De traceerbaarheid van het gebruik van de authenticatiemiddelen op applicatie niveau
- Autorisatie staat in voor:
- Validatie van de toegangen van de gebruiker op basis van de toegekende rechten aan het authenticatiemiddel
- Deze validatie kan op verschillende manieren worden ingeregeld, centraal, individueel of via federatie modellen.
- Active Directory, LDAP
- Host (lokale groepen/rollen op operating systeemniveau)
- Middleware (Databasesystemen)
- ACM
- Technologie gerelateerde access controles
- Binnen de toepassing zelf, als configuratie of in de applicatie code

3.2.3. Logbeheer

- Het log beheer staat in voor het verzamelen en bewaren van audit trails, informatie waarmee (beheers) activiteiten kunnen worden gecontroleerd en gereconstrueerd
- Het logbeheer beschrijft de volledige lifecycle van de log informatie
- Het logbeheer voorziet in de verzameling, centralisatie en eventuele archivering van de log informatie
- Het logbeheer bewaakt de integriteit tijdens de volledige levenscyclus log informatie
- De technische behoeften die toelaten om op aangepaste wijze log informatie te verzamelen worden beschreven als functionele behoeften in het configuratiebeheer van de individuele toepassing of generieke platformen
- Het logbeheer vormt de basis voor de risico rapportering
- Log informatie kan voorkomen op verschillende infrastructuurcomponenten of op componenten met een verschillende beheer context. Om correlatie tussen deze bronnen mogelijk te maken zullen deze bronnen centraal moeten toegankelijk moeten worden gemaakt teneinde correlatie van deze bron informatie mogelijk te maken
- Het resultaat van deze (geautomatiseerde) correlatie zal gebruikt worden als risico rapportering

3.2.4. Risicorapportering

- De operationele risico rapportering (KRI) laat de organisatie toe om op een structurele uniforme manier de belangrijkste operationele risico’s in kaart te brengen en op te volgen in het risico beheer
- Deze rapportering gebruikt de operationele informatie uit processen en de log informatie uit de technische platformen en combineert deze op basis van de verwerkingslogica tot bruikbare rapporten

3.2.5. Het proces

Voorbeeld: HFP PAM Bouwsteen