Uitvoering autorisatiebeleid politie 2016-2020

‘naar een nieuwe autorisatiesystematiek’

Auteur: project autorisatiemodel politie (team beleid en implementatie)

Status: concept

Versie 1.1

20 juni 2016

Rubricering: politie intern (groen)

Versiebeheer

Het autorisatiebeleid 2015-2020 is ontwikkeld door het team beleid en implementatie van het project autorisatiemodel politie ([redacted], [redacted] en [redacted]).

Versie	Versie delen	Samenvatting van de aanpassing
0.1	19-11-2015	Initiële versie, bespreking team
0.2	24-11-2015	Verwerken opmerkingen n.a.v. review
0.3	21-12-2015	Eindredactie
0.4	04-04-2016	Revisie en aanvullingen n.a.v. ontwikkelingen aangegeven door [redacted] (dir. IV) en [redacted] (IM FB)
1.0	21-04-2016	Laatste tekstuele verbeteringen na afstemming met [redacted] (dir. IV) en [redacted] (IM FB)
1.1	20-06-2016	Op verzoek van het MT-CIO zijn voor zover mogelijk en noodzakelijk de begripsdefinities van Wpg-gerelateerde begrippen gehanteerd conform de ‘Leidraad opstellen begripsdefinities’ (v0.9). Termen en begrippen en Bijlage 1 zijn tekstueel aangepast

©2016 Politie, all rights reserved.
Niets uit deze uitgave mag worden verveelvoudigd, op geautomatiseerde wijze opgeslagen of openbaar gemaakt in enige vorm of op enigerlei wijze, hetzij elektronisch, mechanisch, door fotokopieën, opnamen of enige andere manier, zonder voorafgaande schriftelijke toestemming van de Politie.

Distributie en geraadpleegde personen

Versie	Verzend datum	Naam, afdeling en functie
0.1	19-11-2015	Teamleiders van het project autorisatiemodel
0.2	24-11-2015	Teamleiders van het project autorisatiemodel, projectleiding, leden stuurgroep autorisatiemodel, waaronder de CISO en de GA
0.3	21-12-2015	Teamleiders van het project autorisatiemodel, projectleiding, CISO en de GA
0.4	04-04-2016	Teamleiders van het project autorisatiemodel, projectleiding, CISO, de GA, de stuurgroep autorisatiemodel en sr. functioneel beheerder
1.0	21-04-2016	Teamleiders van het project autorisatiemodel, projectleiding, CISO, de GA, de stuurgroep autorisatiemodel en sr. functioneel beheerder
1.1	20-6-2016	5.1.2.e (GegevensAutoriteit), 5.1.2.e (IAM)

Afkortingenlijst

ABA	Audit Based Access
ABAC	Attribute Based Access Control
AP	Autorisatiebeheer proces
Bpg	Besluit politiegegevens
CIO	Chief Information Officer
CISO	Concern Information Security Officer
FB	Functioneel Beheer
GA	Gegevensautoriteit
HR	Human Resources
IAM	Identity & Access Management
ICT	Informatie en Communicatie technologie
IDU	In-, Door- en Uitstroom
IV	Informatie Voorziening
IM	Informatie Management
KA	Kantoorautomatisering
KC	Korpschef
KL	Korpsleiding
LFNP	Landelijk Functiehuis Nationale Politie
NP	Nationale Politie
PID	Project Initiatie Document
RBP	Referentie Model Bedrijfsprocessen Politie
RBAC	Role Based Access Control
TCI	Team Criminele Inlichtingen
Wbp	Wet bescherming persoonsgegevens
Wpg	Wet politiegegevens

Termen en begrippen

Hierna volgen voor de verschillende termen en begrippen die in het autorisatiebeleid worden genoemd, de betekenissen.

Aandachtsgebied	Een aandachtsgebied is een verbijzondering van een werkterrein, gekenmerkt door een grote verscheidenheid aan onderwerpen, waardoor een specifieke inzet en inbreng geldt. Voor deze inzet kunnen nadere opleiding- en certificeringeisen worden gesteld.
Access management	Access management is het geheel aan beleid, verantwoordelijkheden, processen en hulpmiddelen dat organisaties in staat stelt om de toegang tot en het gebruik van systemen en informatie te faciliteren, beheren en controleren.
Applicatie	Een applicatie is (in de context van het autorisatiebeleid) een computer-programma bedoeld voor eindgebruikers. Ook wel ‘toepassing’ genoemd.
Autoriseren	Autoriseren is het machtigen van personen voor het verrichten van verwerkingshandelingen met gegevens.
Autorisatiematrix	De autorisatiematrix is het overzicht waarin alle actuele autorisatiematrixrollen in relatie zijn gebracht met toegestane gegevens verwerkingshandelingen.
Autorisatiematrixrol	Een autorisatiematrixrol is een rolbenaming ten behoeve van autorisaties, gebaseerd op de combinatie van de toegekende LFNP functie, de feitelijke organisatie eenheid en het vakgebied.
Autorisatiemutatie	Een autorisatiemutatie is iedere handmatige of geautomatiseerde handeling, die een verandering te weeg brengt in bestaande gegevens die betrekking hebben op een autorisatie.
Autorisatieprofiel	Een autorisatieprofiel is de beschrijving van alle verwerkingsrechten die bij één of meerdere autorisatiematrixrollen behoren.
Autorisatiesysteem (stelsel van autorisaties)	Het autorisatiesysteem is het geheel van autorisaties dat onder de verantwoordelijkheid van de Korpschef wordt onderhouden om te voldoen aan de vereisten van zorgvuldigheid en evenredigheid ex artikel 6.1 van de Wpg.
Beheer van matrixrollen	Het beheer van matrixrollen is de zorg en verantwoordelijkheid voor het actueel houden, onderhouden en wijzigen van de autorisatiematrix-rollen en de autorisatiematrix.
De-autoriseren	De-autoriseren is het beëindigen van de machtiging van een persoon voor het verrichten van verwerkingshandelingen met gegevens.
Gegevens	Gegevens zijn (in de context van het autorisatiebeleid) feiten, begrippen en informatie die die in het kader van de uitvoering van een

	taak noodzakelijk kunnen zijn. We onderscheiden hierin politie-gegevens en bedrijfsvoeringsgegevens.
Identificatie	Identificatie van een persoon is een methode, procedure of handeling om vast te stellen dat iemand is wie hij/zij beweert te zijn.
Identity Management	Identity Management is het geheel aan beleid, verantwoordelijkheden, processen en hulpmiddelen dat organisaties in staat stelt om de identificatie en authenticatie van actoren (gebruikers en systemen) te faciliteren, beheren en controleren.
LFNP functie	Een LFNP functie is een functie in het Landelijk Functiehuis Nationale Politie. Voor elke LFNP functie is vastgelegd welke verantwoordelijk-heden, taken, activiteiten en bevoegdheden, welke mate van zelfstandig handelen en welk werk- en denkniveau aan de functie verbonden zijn om de functie naar behoren te kunnen invullen.
Leidinggevende	Een leidinggevende is een medewerker van de politie, die leiding geeft of als plaatsvervanger leiding geeft aan een organisatieonderdeel waarin de politietaak wordt uitgevoerd of aan een organisatieonderdeel waar ondersteunende werkzaamheden aan de politietaak uitgevoerd worden, en als zodanig in het HR systeem is aangemerkt.
Mandateren/ delegeren	Mandateren is iemand de bevoegdheid geven om in naam van een ander te handelen, zonder de daarbij horende verantwoordelijkheid. Bij mandateren worden geen bevoegdheden overgedragen; de mandaat-gever blijft zelf bevoegd. Dit in tegenstelling tot delegeren, wat het overdragen van bevoegd-heden inclusief verantwoordelijkheid inhoudt. Een mandaatgever blijft bevoegd de gemandateerde bevoegdheid zelf te hanteren.
Mutatiegegeven	Een mutatiegegeven is een gegeven met een hoge wijzigings-frequentie.
Organisatie eenheid	Een organisatie eenheid is een formatieve en/of feitelijke plaats in de organisatie waar taken en werkzaamheden worden uitgevoerd.
Permissie	Een permissie is een functionele afbeelding in het IAM van een ‘applicatierol’ in een (doel-)systeem.
Primaire opleidingseis	Een primaire opleidingseis is een opleidingseis zoals benoemd in een LFNP functieprofiel.
Rol	Een rol is … - een samenhangend pakket aan taken die door een of meer personen vervuld kan worden. - een verzameling permissies, benodigd om een samenhangend pakket aan taken die door een of meer personen vervuld kan worden (rol) te kunnen vervullen.
Secundaire opleidingseis	Een secundaire opleidingseis is een opleidingseis die gekoppeld is aan een vakgebied of aan additionele taken.

Stamgegeven	Een stamgegeven is een gegeven welk basisinformatie bevat voor de applicaties waarin het gebruikt wordt. Stamgegeven kennen een (zeer) geringe wijzigingsfrequentie.
Specifieke functionaliteit	Specifieke functionaliteit is een verbijzondering van een vakgebied, door – direct in operationeel verband toe te passen – vereiste expliciete specialistische inzet en inbreng door gebruikmaking van specifieke (hulp) middelen en/of geweldsmiddelen, waarbij uitgesproken specialistische vaardigheden en deskundigheid aan de orde is.
Toegangs-voorwaarde	Een toegangsvoorwaarde is (in de context van het autorisatiebeleid) een voorwaarde waaraan voldaan moet worden om toegang tot gegevens te verkrijgen.
Vakgebied	Een vakgebied is een verzameling van specifieke taken die binnen een LFNP functie ten behoeve van een organisatie eenheid worden uitgevoerd. Het betreft een clustering van in essentie gelijkgerichte activiteiten en beoogde effecten op basis van voor dat vakgebied geldende processen.
Werkterrein	Een werkterrein is een verbijzondering van een vakgebied, waarvoor specifieke inzet en inbreng geldt.

Inhoudsopgave

1. Inleiding

Deze regeling dient als onderlegger van het autorisatiebeleid politie 2015 – 2020. Op het moment van het vaststellen van het autorisatiebeleid zijn logischerwijs nog niet alle elementen en principes binnen de organisatie in werking gebracht. Deze uitvoeringsregeling dient als basis om het autorisatiebeleid uiterlijk eind 2019 meetbaar gerealiseerd te krijgen en beschrijft hoe het autorisatiebeheer in uitvoering wordt genomen.

Er is één centraal aangestuurd autorisatiebeheerproces. Dat proces valt onder verantwoordelijkheid van de daartoe aangewezene van de korpsleiding (KL): de verantwoordelijke namens de korpschef (KC).

De lijn die in gang is gezet met de inwerkingtreding van de Identity & Access Management (IAM) tool, namelijk ‘rol gebaseerd’ toekennen van autorisaties, wordt gecontinueerd. Een medewerker krijgt één of meerdere autorisatiematrixrollen toegekend op basis van de feitelijke werkzaamheden die volgen uit zijn/haar functie conform het Landelijk Functiehuis Nationale Politie (LFNP), organisatorische plaats en de daarbij behorende taakstelling. Aan die rol(len) zit(ten) een reeks van permissies ten aanzien van toegang en verwerking van gegevens vast.

De vastgestelde bevoegdheden per autorisatiematrixrol zijn op noodzaak beoordeeld - nodig voor de taak van de medewerker - en geaccordeerd op basis van een formeel besluit van de daartoe aangewezen portefeuillehouder.

2. Applicaties en toegang tot gegevens

De actuele wet- en regelgeving en korpsdoelstellingen in het bijzonder aangaande het delen van informatie worden geborgd in het verwervings- en ontwikkelproces van de applicaties die toegang geven tot gewenste gegevens. Belangrijke aandachtspunten zijn onder meer normen als voor vertrouwelijkheid, beschikbaarheid, integriteit en controleerbaarheid van gegevens.

Privacy by design geldt als leidend principe. Dit houdt in dat geborgd wordt dat de beginselen van de privacy bescherming zo veel mogelijk worden ingebouwd in de informatievoorziening. Het moet ook uitgangspunt zijn bij de opbouw van de gegevens tot gegevenssets die via de applicaties toegankelijk worden gemaakt.

De toegangsmogelijkheden tot gegevens worden in de applicaties geautomatiseerd afgebakend op basis van een gefundeerde voorafgegane verkenning ten aanzien van de behoeftestelling: welke gegevens heeft men nodig voor welke taak.

In het kader van functiescheiding zijn wijzigen en goedkeuren niet verenigbaar, hetzelfde geldt voor toevoegen en goedkeuren als wel verwijderen en goedkeuren.

Richtinggevend is dat autorisatiegegevens voor de uitvoering van het autorisatiebeleid drie jaar bewaard moeten worden. Bewaren betekent in dit verband ‘het beschikbaar houden’ voor het kunnen controleren van en toezien op alle vastgestelde afspraken met betrekking tot het uitvoeren van het autorisatiebeleid en het voldoen aan wet- en regelgeving, alsmede voor de evaluatie van het stelsel van autorisaties. Dit met inachtneming van de wettelijke termijnen die van toepassing zijn op het bewaren, verwijderen en vernietigen van persoonsgegevens. Welke gegevens bewaard moeten worden alsmede de bewaarperiode kunnen in een regeling nader beschreven worden.

Met het oog op toezicht moet er naar worden gestreefd dat geautomatiseerd eventueel evident afwijkend gedrag in het bevragen van gegevens, kan worden herkend. Het gaat om gebruik van de applicatie die kunnen wijzen op een onoordeelkundig of op beslist ongewenst gebruik van de gegevens. De criteria waarop controle mogelijk is moeten worden benoemd.

3. Informatiebeveiliging

De Concern Information & Security Officer (CISO) wordt namens de verantwoordelijke belast met het voorbereiden en inrichten van het stelsel van autorisaties. Concreet houdt dit in dat op strategisch niveau de CISO niet alleen verantwoordelijk is voor een ingerichte en goed werkende autorisatiesystematiek maar dat deze geborgd is, nageleefd wordt en continu verbeterd wordt.

De CISO rapporteert over de voortgang van het realiseren van het autorisatiebeheerproces aan de Chief Informatie Officer (CIO).

De CISO rapporteert over output en outcome van het autorisatiebeheerproces aan de verantwoordelijke.

Als uitvloeisel van een goed werkende geborgde autorisatiesystematiek die gemonitord en continu verbeterd wordt, worden mogelijke handelingen die geautomatiseerd gedetecteerd zouden kunnen worden die zouden kunnen wijzen op onoordeelkundig of evident onjuist gebruik van gegevens met een mogelijk risico voor de informatievoorziening, gedefinieerd.

Hetzelfde geldt voor het definiëren van beveiligings issues die zich in het autorisatiebeheerproces kunnen voordoen en de wijze van rapporteren over de issues.

De verificatie van het effectief en efficiënt werken van de autorisatie systematiek wordt periodiek uitgevoerd door het team informatiebeveiliging en is een operationele verantwoordelijkheid van IM. De aan de autorisatiesystematiek gekoppelde verschillende uitvoeringsfuncties rapporteren periodiek over de voortgang aan en stellen rapportages op voor de CISO.

4. Gegevensbeheer

Het stelsel van autorisaties dat wordt doorgevoerd mag geen afbreuk doen en moet waar mogelijk bijdragen aan het borgen van de kwaliteit van gegevens waar het gaat om juistheid, volledigheid, beschikbaarheid en levensduur alsmede aan nut, noodzaak, rechtmatigheid et cetera van het gebruik van de gegevens.

Waar in de verwerking van gegevens een zodanige onduidelijkheid ontstaat zoals leemtes, overlappingen en ontbreken van eenduidige betekenis die de geautomatiseerde toekenning van autorisatierechten in de weg staat, zal deze onduidelijkheid moeten worden weggenomen.

5. Leidinggevenden

De leidinggevenden geven, voor zover zij daartoe door of namens de KC zijn gemandateerd, de aan hen toegewezen medewerkers tijdelijk specialistische autorisaties voor verwerking van gegevens die de betrokken medewerker nodig heeft om de aan hem/haar opgedragen specialistische taak te kunnen uitvoeren.

De leidinggevenden zijn verantwoordelijk voor het de-autoriseren van een medewerker in geval van uitdiensttreding, buiten functie stelling en in voorkomende gevallen bij langdurig verlof, ziek of afwezigheid en functiewijziging.

6. Medewerkers

De achilleshiel van autoriseren is het vaststellen van de juistheid van identiteit van personen die uiteindelijk toegangsrechten tot de gegevens krijgen.

HR is verantwoordelijk voor de juistheid, volledigheid en tijdigheid van personeelsgegevens alsmede het daaraan gekoppelde kwaliteit verbeterproces.

HR rapporteert over het kwaliteit verbeterproces aan de CIO, de CISO en IM vooral waar het gaat om de effecten op het autorisatieproces.

De verantwoordelijkheid voor het vaststellen van de identiteit en juistheid van onderliggende documenten met betrekking tot opleidingen en werkverleden ligt bij Human Resources (HR).

Iedere medewerker doorloopt binnen de organisatie een aantal processen:

- instroom, betreft de indiensttreding van een medewerker;
- doorstroom, betreft de verplaatsing van een medewerker binnen de organisatie;
- uitstroom, betreft het verlaten van de organisatie door de medewerker;
- mutaties, betreft wijzigingen in de basisgegevens van een medewerker waardoor het profiel wijzigt.

De life cycle van autorisaties voor de medewerker wordt vastgelegd in het in-, door- en uitstroom (IDU) proces. Dit proces van HR zorgt voor de juiste, volledige en actuele medewerkers informatie.

Het beschikken over volledige, juiste en actuele medewerker gegevens vormt voor elke ondersteunende afdeling de basis om haar werkzaamheden uit te voeren.

Screeningseisen voor een functie worden vastgesteld door Veiligheid, Integriteit en Klachten (VIK). De screening moet succesvol zijn verlopen voordat de mutatie hiertoe in het ondersteunend personeelssysteem van HR (thans Beaufort NP) wordt vastgelegd, zowel bij in- als doorstroom. Hetzelfde geldt voor specifieke functie eisen. Wanneer de leidinggevende medewerkers gegevens met het oog op specialistische taken muteert is het de verantwoordelijkheid van de leidinggevende dat de medewerker voldoet aan alle opleidings- en screeningseisen.

Om de verantwoordelijkheden voor gegevens eenduidig in de organisatie te kunnen toewijzen, is voor het muteren van gegevens een zodanig consistente set beheertaken aanwezig. Deze beheertaken borgen dat mutatiebevoegdheden eenduidig toegewezen kunnen worden. De beheertaken zijn de verantwoordelijkheid van HR en geven aan welke mutaties de leidinggevende mag uitvoeren en welke bij HR liggen.

Toekenning van de noodzakelijke autorisaties benodigd voor de betreffende functie van de medewerker wordt voldaan via dynamische koppeling van de betreffende rol(len). De medewerker wordt door HR bij instroom en doorstroom voorzien van de correcte LFNP-functie. Dit zorgt, in combinatie met de juiste organisatorische plaats van de medewerker en het vakgebied, voor de automatische koppeling van de juiste rol(len). Wanneer de medewerker doorstroomt binnen de organisatie worden de bij de oude functie behorende toegekende rol(len) ingetrokken en tegelijk de bij de nieuwe functie behorende rol(len) toegekend. Wanneer de medewerker uitdienst treedt worden dezelfde rol(len) ook automatisch verwijderd.

Het actuele beleid voor toegang tot accounts en de kantoorautomatiseringsomgeving (KA) door medewerkers die langdurig ziek zijn of afwezig, bijvoorbeeld in het kader van detachering buiten de organisatie zijn, blijft gehandhaafd. De toegang wordt opgeschort voor de door HR opgegeven duur van afwezigheid.

Waar het gaat om toegang tot accounts en de KA omgeving door medewerkers die gebruik maken van een vervroegde uitreed- of herplaatsingsregeling, moet per regeling door HR worden aangeven op welk moment het verantwoord is de toegang voor de KA omgeving te beëindigen.

7. Partners

Een partner is een nationale en internationale organisatie met een wettelijke taak op het gebied van veiligheid en justitie, waarmee de politie operationeel samenwerkt. Ten aanzien van partners is het volgende relevant.

Binnen de politie komt een uniform proces waaraan partnerorganisaties zijn gehouden wanneer zij direct toegang mogen verkrijgen tot gegevens van de politie.

Voor zover het hier gaat om partners die vallen binnen het perspectief van de beleidskader 'IV-dienstverlening aan partners'[1] wordt de hierin opgenomen beleidslijnen aangehouden.

Voor partners kunnen voor de toegangsverlening tot politiesystemen, tot een minimum beperkt, aanvullende eisen gelden. Deze eisen worden in een nadere regeling vastgelegd. Degene die deze aanvullende eisen goedkeurt zorgt voor de inbedding daarvan in de autorisatiesystematiek en realiseert relevante rapportagemogelijkheden.

Er moet in het kader van het autorisatiebeleid worden onderscheiden naar rechtstreeks verstrekking waarbij de ontvanger kan bepalen wat deze verwerkt uit de politiesysteem òf waarbij ontvanger en verstrekker (de politie) op voorhand samen hebben bepaald wat verwerkt kan worden. Dit in verband met de te onderscheiden bepalingen van de Wpg ter zake.

Het autorisatiebeheer voor externe partners moet vanuit oogpunt van verbeterde beheersbaarheid bij alle regionale eenheden en de landelijke eenheid op eenduidige wijze worden toegepast. Uitzonderingen hierop mag alleen met toestemming van de eigenaar van het proces autorisatiebeheer. Het programma Dienstverlening Partners heeft het voortouw bij de totstandkoming van de besluitvorming met derden.

De rechtstreeks toegang van partners moet dezelfde administratieve weg volgen als voor eigen medewerkers. Dit betekent dus in de huidige structuur dat de betreffende medewerker van de partnerorganisatie opgevoerd wordt binnen het personeelssysteem van de politie (Beaufort NP) om op deze manier deze persoon toegangsrechten te geven.

Voor het registreren, bewaken en borgen van de vereisten voor toegangsrechten voor partners staat centraal de eis dat bij de partnerorganisatie één aanspreekpunt/loket zal zijn voor het autorisatiebeheer in de relatie tot autorisaties van de politie. Uiteraard kunnen partners een samenwerkingsverband aangaan om tot één loket te komen.

De partner wordt verplicht correcte gegevens via een centraal punt aan te leveren, via één landelijk eenduidig aanvraagproces dat voldoet aan de eisen die door de politie daaraan zijn gesteld. De partner organisatie is ook verantwoordelijk om in de eigen administratie te borgen dat vastgelegd is dat de betreffende medewerker de toegangsrechten van de politie heeft verkregen, zodat bij wijziging van functie of uitdiensttreding van de medewerker dit ook kan worden doorgegeven aan de politie. Dit is van belang in het geval dat ten behoeve van een audit de actualiteit van de aantallen zal worden beoordeeld.

In principe worden de volgende eisen in acht genomen aan de te autoriseren medewerker van de partner organisatie.

[1] Beleid van 27 februari 2014

De medewerker:

- voldoet aan de opleidings- en screeningseisen zoals gesteld voor de betreffende autorisatiematrixrol(len), inclusief herhalingen, tenzij de wet anders bepaalt. De verantwoordelijkheid voor het naleven hiervan ligt bij de partnerorganisatie;
- krijgt toegang voor een afgebakende periode en de daarbij behorende einddatum wordt ook bij invoer geregistreerd;
- verliest zijn/haar toegangsrecht als deze voor een bepaalde tijd, in principe een kortere periode dan geldig is voor internen, er geen gebruik van heeft gemaakt. Het account zal worden gedeactiveerd.

Voor de organisatie van de partner geldt dat deze:

- gehouden is aan het autorisatiebeleid geldend binnen de politie;
- bij uitdiensttreding het administratieve onderdeel, dat het autorisatieproces bij de externe organisatie uitvoert bij de politie uiterlijk één maand voor uitdiensttreding hierover informeert;
- toestaat dat de politie het recht krijgt een controle op de persoon te kunnen uitvoeren waar het gaat om de gemaakte afspraken met de politie ten aanzien van het autorisatiebeheer volgens het ‘right to audit’ principe. Daarnaast moet de partnerorganisatie toestaan dat de politie de noodzakelijkheid van toegang verifieert en weegt.

Van alle afzonderlijke samenwerkingsverbanden moet in beeld worden gebracht wat precies de status is van de samenwerking met deze partijen en hoe dat over het gehele land op eenduidige wijze kan worden uitgerold.

Hierbij moet gelet worden op mogelijke afspraken die in de voormalige 26 korpsen zijn gemaakt met deze partijen met inachtneming van de eisen en wensen van de partners.

8. Autorisatiebeheer

Tot de belangrijkste taken van de proceseigenaar behoren, naast het vaststellen van het proces, het vaststellen van de autorisatiematrices en autorisatieprofielen evenals het vaststellen van rapportages over de voortgang van de diverse stappen in het proces.

Het goedkeuren van de autorisatiematrixrollen is een aangelegenheid van de portefeuillehouder autoriseren[2] die daartoe eigenaren op strategisch niveau heeft aangewezen. Uit oogpunt van beheersbaarheid moet het aantal autorisatiematrixrollen beperkt blijven, om de eigenaren niet te veel te belasten met beslismomenten over de inhoud van elk afzonderlijke autorisatiematrixrol.

De leidinggevende komt een bijzondere bevoegdheid en verantwoordelijkheid toe in het proces van het autorisatiebeheer. Aan de leidinggevende van elke organisatorische eenheid komt immers de uiteindelijke verantwoordelijkheid toe om er op toe te zien dat de medewerkers van zijn/haar organisatie-eenheid voldoende kunnen beschikken over de juiste autorisaties om hun taken naar behoren te kunnen uitvoeren.

Is dat naar zijn/haar oordeel niet het geval dan komt de leidinggevende in het verlengde hiervan de bevoegdheid toe om op individueel niveau correcties en/of aanvullingen aan te kunnen aanvragen op de daadwerkelijk beschikbaar gestelde autorisaties en autorisatieprofielen. De aanvragen worden via de eigen lijn ingediend bij desbetreffende landelijke platformen. FB heeft ten aanzien van de verzoeken een adviesfunctie. De door de platformen vastgestelde aanpassingen worden de desbetreffende eigenaren ter goedkeuring aangeboden. De wijzigingen en/of aanvullingen worden via de landelijke platformen ingevoerd en gecommuniceerd.

Het stelsel van autorisaties dient landelijk beheerd te worden. De Informatie en Communicatie Technologie (ICT) toepassing die de organisatie daartoe heeft verworven worden de gegevens centraal vastgelegd. Het beheer daarop kan centraal of decentraal plaatsvinden. Hiervoor is een autorisatiebeheer proces vastgesteld.

De algemene doelstelling van autorisatiebeheer is het op een beheerste, gecontroleerde en uniforme wijze de juiste persoon toegang verlenen tot de juiste gegevens, waarbij ‘delen tenzij wet- en regelgeving dat verbiedt’ in acht wordt genomen.

HR draagt er voor zorg en is verantwoordelijk voor de juistheid van gegevens met betrekking tot de identiteit van personen die ingevoerd worden in het personeelssysteem (Beaufort NP).

De inhuurdesk draagt zorg en is verantwoordelijk voor de juistheid van gegevens met betrekking tot de identiteit van inhuurmedewerkers die via HR in het personeelssysteem (Beaufort NP) worden ingevoerd.

De Relatiedesk van Service Level Management (SLM) draagt zorg en is verantwoordelijk voor de juistheid van gegevens met betrekking tot de identiteit van medewerkers van externen en ketenpartners, die via HR in het personeelssysteem (Beaufort NP) worden ingevoerd.

Autorisatiebeheer draagt zorg en is verantwoordelijk voor het actief rapporteren over opvallende en/of afwijkend lijkende autorisaties en –trends.

[2] Zie hoofdstuk 9 Governance

9. Governance

Met governance wordt de sturing over de keten bedoeld. Deze is conform het governance document van de oplosgroep, geaccepteerd door de Dienst IM, als volgt georganiseerd.

CISO

De CISO ziet er op toe dat de beschikbaarheid, exclusiviteit en integriteit van de door de politie gebruikte gegevens en informatie gewaarborgd is en blijft, conform wet- en regelgeving en beleid, zodanig dat de te bereiken doelen van de NP maximaal ondersteund worden.

Autoriseren is een van de middelen en/of werkwijzen om de beschikbaarheid, exclusiviteit en integriteit van de politiegegevens en informatie in goede banen te houden.

De CISO is een functie binnen de Directie IV.

Portefeuillehouder autoriseren

De portefeuillehouder autoriseren is verantwoordelijk voor de portefeuille autoriseren.

De portefeuillehouder zorgt dat een autorisatiebeleid opgesteld wordt en dit gerealiseerd wordt conform wet- en regelgeving en beleid zodanig dat de te bereiken doelen van de NP maximaal ondersteund worden.

Het portefeuillehouderschap autoriseren is belegd bij de politiechef van de eenheid Amsterdam.

Overkoepelend procesverantwoordelijke

De Dienst IM is overkoepelend procesverantwoordelijke voor het autorisatieproces. De overkoepelend procesverantwoordelijkheid is belegd bij het DIM MT lid die autorisaties in zijn/haar portefeuille heeft.

De overkoepeld procesverantwoordelijke ziet er namens de portefeuillehouder autoriseren en het MT PDC op toe dat het IDU autorisatieproces en meer/minder rechten over de gehele voortbrengingsketen effectief functioneert, en effectief blijft functioneren, binnen de kaders gesteld door de portefeuillehouder.

Efficiëntie is initieel niet een doel maar een streven. Continue verbetering is initieel niet een doel maar een middel.

De overkoepelend procesverantwoordelijke laat zich gevraagd en ongevraagd informeren over - (effectiviteit van) de werking van het autorisatieproces, de risico's en de - mogelijkheden tot verbetering.

De overkoepelend procesverantwoordelijke informeert de portefeuillehouder, de CISO en het MT PDC gevraagd en ongevraagd over het autorisatieproces. Tenzij anders afgesproken, is er geen periodieke verantwoordingsafstemming.

De overkoepelend procesverantwoordelijke zet binnen de kaders gesteld door de portefeuillehouder en het MT PDC de tactische koers uit voor het autorisatieproces (inclusief de governance), voor de middellange termijn en voor de langere termijn.

De overkoepelend procesverantwoordelijke initieert elk jaar een doorlichting en elk derde jaar een interne audit van aspecten van het autorisatieproces die conform beleid geaudit moeten worden, risicovol zijn alsmede onderkende of vermoedelijke zwakke plekken.

De overkoepelend procesverantwoordelijke bewaakt dat elke processtap een actief betrokken processtap verantwoordelijke kent. Indien dit niet het geval is, vraagt de overkoepelend procesverantwoordelijke aan het relevante Diensthoofd om deze situatie te rectificeren.

De overkoepelend procesverantwoordelijke deelt en delegeert taken, bevoegdheden en verantwoordelijkheden om operationele targets te behalen, afgestemde planningen te realiseren en hierover tijdig te rapporteren met en/of aan de processtap verantwoordelijken.

Processtap verantwoordelijke

De processtap verantwoordelijke zorgt dat het autorisatieproces binnen zijn of haar organisatieonderdeel doeltreffend functioneert en blijft functioneren, binnen de kaders gesteld of doorvertaald door de overkoepelend procesverantwoordelijke.

De processtap verantwoordelijke ziet er op toe dat afgesproken plannen en targets met betrekking tot het autorisatieproces tijdig gerealiseerd worden.

De processtap verantwoordelijke ziet er op toe dat alle relevante medewerkers in zijn/haar afdeling of team goed geïnstrueerd zijn, de juiste tools en attitude hebben, adequaat geïnformeerd worden over het autorisatieproces.

De processtap verantwoordelijke laat zich gevraagd en ongevraagd informeren over de (effectiviteit van) werking van het autorisatieproces in zijn/haar afdeling of team, alsmede aanpalende afdelingen en teams, risico's en mogelijkheden tot verbetering.

De processtap verantwoordelijke initieert elk jaar een doorlichting en elk derde jaar een interne audit van aspecten van het autorisatieproces in zijn/haar afdeling of team die conform beleid geaudit moeten worden, risicovolle aspecten, onderkende of vermoedde zwakke plekken.

De processtap verantwoordelijke stelt elke drie maanden, of frequenter indien afgesproken, een rapportage op voor de overkoepelend procesverantwoordelijke over het autorisatieproces in zijn/haar afdeling of team met betrekking tot de performance ten opzichte van de indicatoren, een verbetervoorstel als een doel niet behaald wordt, risico's, relevante veranderprojecten en veranderinitiatieven in de eigen dienst en daarbuiten.

Daarnaast informeert de processtap verantwoordelijke de overkoepelend procesverantwoordelijke gevraagd en ongevraagd over het autorisatieproces in zijn/haar afdeling of team, alsmede aanpalende afdelingen en teams, tijdens het periodieke Autorisatie governance-overleg en ad hoc, incidenteel zodra een afwijking of risico wordt geconstateerd.

De processtap verantwoordelijke waakt dat binnen zijn/haar afdeling of team, en binnen zijn/haar dienst, geen veranderprojecten of -initiatieven voorbereid of uitgevoerd worden die een (positief of negatief) effect kunnen hebben op de werking van een of meerdere stappen van de autorisatie voortbrengingsketen – zonder degelijke afstemming.

Een dergelijke verandering (van proces, data, bemensing en/of tooling) mag alleen uitgevoerd worden als de overkoepelend procesverantwoordelijke en alle processtap verantwoordelijken tijdig geïnformeerd zijn en alle processtapverantwoordelijken expliciet akkoord gegeven hebben

omdat de verandering hun processtap niet treft, of de verandering treft hun processtap wel maar ze gaan akkoord met de verandering en de consequenties van de verandering.

De processtap verantwoordelijke laat de projectleider of coördinator van de verandering de degelijke afstemming realiseren.

Processtap verantwoordelijkheid is belegd bij van elke dienst die bijdraagt aan de autorisatie voortbrengingsketen en wordt aangewezen door het diensthoofd.

10. Deactivering

Accounts en autorisaties van een medewerker moeten binnen bepaalde kaders gedeactiveerd respectievelijk gedeautoriseerd en verwijderd kunnen worden.

Het is mogelijk om in bepaalde situaties zoals bij een intern onderzoek of bij hoge urgentie de autorisaties van een medewerker door de leidinggevende te direct ontnemen via een zogenaamde noodknop functie. De noodknop kan 24/7 'real time' worden geactiveerd.

Indien de noodzaak om toegang te ontnemen niet meer aanwezig is, moet het voor de betreffende medewerker mogelijk zijn de autorisaties op de eerste werkdag na dit besluit, weer beschikbaar te krijgen.

In het navolgende schema zijn vier scenario's gegeven met daarbij behorende de-autorisatie termijnen.

Scenario's	De-autoriseren
Geen gebruik na creatie	100 dagen na geen gebruik
Geen gebruik laatste 3 maanden	100 dagen na laatste gebruik
Regulier uit dienst	1 dag na einde contractdatum
Prioriteit Noodstop	binnen 1 uur na verzoek van leidinggevende

Voor alle vier scenario's geldt dat de autorisaties worden verwijderd conform de actuele richtlijn zoals die van toepassing is op door- en uitstroom van medewerkers.

11. Controle en toezicht

Op het moment van het vaststellen van het autorisatiebeleid zijn logischerwijs nog niet alle elementen en principes binnen de organisatie in werking gebracht. Om die reden stelt IM jaarlijks een plan op welke specifieke doelen ten aanzien van het autorisatiebeleid bereikt moeten gaan worden. In het plan wordt aangegeven op welke wijze en met welke frequentie de voortgang ten opzicht van bedoeld plan wordt gemeten. Het plan wordt de CISO voorgelegd.

Daarnaast worden periodieke controles in ieder geval jaarlijks uitgevoerd voor meerdere doeleinden. Het gaat daarbij om:

- kunnen voldoen aan de vraag van informatie (gegevensvraag) voor interne en externe auditoren;
- kunnen aantonen dat het proces van monitoring effectief is en efficiënt wordt toegepast;
- kunnen aantonen dat de logging die over de verschillende systemen plaatsvindt effectief is en efficiënt wordt toegepast;
- aantonen van volwassenheidsniveau van het autorisatieproces;
- aantonen dat de ‘system development life cycle’, project management principes en ‘information security controls’ effectief zijn en efficiënt worden toegepast.

Controles moeten de doelstellingen van de organisatie ondersteunen of verplicht zijn gesteld door de wetgever.

De controles kunnen zowel structureel als ad hoc zijn. Ze kunnen repetitief worden gedaan. Een continue monitoring kan worden overwogen waarmee volautomatisch op vooraf geplande intervallen, rapportage en meldingen worden gedaan aan de hand van vooraf ingestelde drempels.

Algemeen geldend uitgangspunt ten aanzien van controle en toezicht is dat elke uitvoerende en bij de autorisatiesystematiek betrokken functie geacht wordt periodiek te rapporteren over de aangewezen taken en verantwoordelijkheden op het naast hoger liggende verantwoordelijke en de CISO.

Er zal naar gestreefd worden om zoveel mogelijk schendingen van het autorisatiebeleid af te vangen met geautomatiseerde monitoring. Dat betekent dat zo spoedig mogelijk met de beheerders van de politiesystemen overeenstemming moet worden bereikt over het zo veel als mogelijk invoeren van daarop afgestemde intelligentie in deze systemen.

Het signaal moet aanleiding geven om de verwerkingshandeling achteraf te toetsen aan de vraag of het nodig was voor de uitoefening van de politietaak van degene die de verwerking heeft gedaan.

Daarnaast zal door steekproeven worden gecontroleerd. De frequentie van de steekproef wordt mede ingegeven door wat bij eerdere steekproeven is geconstateerd. Worden er weinig omissies ontdekt dan kan verder worden gegaan op een lage frequentie. Worden er daartegen veel onjuistheden of andere omissies gezien dan worden op een hogere frequentie de steekproefsgewijze controles gecontinueerd.

Vooralsnog kan worden volstaan met een eerste uitgebreide steekproef op grond waarvan in redelijkheid kan worden bepaald of in het vervolg intensief of beperkt kan worden gecontroleerd.

De CISO is aanspreekpunt en is door de KC gemandateerd, voor het borgen, bewaken van alsmede rapporteren en adviseren over de processen en resultaten van de controle en toezicht op het systeem van autorisaties.

Voor het beheersen, door middel van controle en toezicht, van het autorisatieproces wordt Audit Based Access (ABA)[3] aangehangen. Dit is een bewezen 'best practice', waarbij de ervaring daarmee bij veel grote organisaties actief worden meegenomen.

Daarbij geldt dat het aan volgende moet zijn voldaan.

- Sprake moet zijn van een één eenduidig proces van in-, door- en uitstroom van personen met daaraan gekoppelde autorisaties.
- Eén loket, d.w.z. een centrale unit waar alle gegevens omtrent het beheer en de verwerking van autorisaties wordt geadministreerd met als doel een éénmalige vastlegging van gegevens.
- Eigenaarschap is belegd voor de verschillende autorisatieprofielen en afzonderlijke gegevens.
- Bij wijzigen van het gebruik of het nieuw toepassen van een gegevens gekoppeld aan een autorisatieprofiel en/of specials, moet de relevante proceseigenaren worden gevraagd voor akkoord op dit verzoek.

Er moet naar worden gestreefd dat de bij autorisatie gegeven permissies ook te vertalen zijn naar criteria waarop controle mogelijk is. Een bekend voorbeeld is dat door medewerkers in politiesystemen wordt gezocht naar een bekende Nederlander die wegens vermeend crimineel gedrag in het nieuws komt.

De CISO en de GA moeten de bedrijfsvoering en operatie criteria laten identificeren waarop het mogelijk wordt dat medewerkers die binnen hun taak hier niets mee van doen hebben, worden gesignaleerd.

De gegevens die voor controle en toezicht beschikbaar moeten blijven, moeten worden geïdentificeerd. Het is van belang dat de organisatie aangeeft welke controles zij willen en daaruit wordt afgeleid welke gegevens bewaard moeten worden om daartoe een controle mechanisme op te zetten. Deze moeten voor de duur dat de controle en toezicht zich volgens een daartoe opgestelde planning kan voordoen, beschikbaar blijven. Enerzijds gaat het hier om de concrete verwerking die is gedaan, zoals opslaan, raadplegen, veredelen en gebruiken. In ieder geval alles wat onder de definitie van verwerken valt volgens de Wet politiegegevens (Wpg). Anderzijds gaat het hier om de identiteit van degene die de verwerking heeft gedaan (identificatie). Het gaat dan om de combinatie van naam en in welke hoedanigheid/functie de betreffende medewerker de verwerking heeft verricht, wat valt onder het regiem van de Wet bescherming persoonsgegevens (Wbp).

De bewaartermijnen in het kader van het autorisatiebeleid kunnen goed samen gaan met de registratieverplichtingen in het kader van de Wpg. De Wpg geeft aan hoe lang gegevens bewaard mogen worden ten behoeve van de privacy audit op de uitvoering van de politietaak. Deze termijnen kunnen ook worden gehanteerd voor het autorisatiebeleid. Bijkomend voordeel is dat de privacy audit ingevolge de Wpg[4] samen kan vallen met audit op het autorisatieregime, wat uit kostenperspectief voordelig is.

[3] zie de toelichting in bijlage van het autorisatiebeleid politie 2015-2020
[4] artikel 33 Wpg

Elk beleidsvoerend en –makend organisatieonderdeel is belast met de interne controle op de werkprocessen met het doel de KL te adviseren over de werking van het stelsel van autorisaties op basis van nader vast te stellen criteria voor output en outcome meting.