Autorisatiebeleid politie 2016-2020

‘naar een nieuwe autorisatiesystematiek’

Auteur: project autorisatiemodel politie (team beleid en implementatie)

Status: definitief

Versie 1.0

27 januari 2016

Rubricering: politie intern (groen)

Versiebeheer

Het autorisatiebeleid 2016-2020 is ontwikkeld door het team beleid en implementatie van het project autorisatiemodel politie ([redacted], [redacted] en [redacted]).

Versie	Versie datum	Samenvatting van de aanpassing
0.1	04-12-2014	Initiële versie, bespreking team, document Identity & Access Management Functionaliteiten, document deactiveren, document Minicompetitie-Offerteaanvraag IAM software en diensten
01.0	06-05-2015	Bespreekversie voor de projectmanager en teamleiders
02.0	02-06-2015	Bespreekversie voor de projectmanager onder meer ter behandeling in de stuurgroep en ter afstemming met stakeholders
02.1	16-06-2015	Concept versie ter bespreking in de stuurgroep
02.2	27-08-2015	Eind review
03	07-09-2015	Voor commentaar naar de Stuurgroep BI
04	30-10-2015	Scheiding aangebracht in beleid en uitvoeringstrategie n.a.v. review GA en CISO
05	09-11-2015	Verfijning randvoorwaarden en uitgangspunten
06	15-12-2015	Eindredactie
1.0	27-01-2016	In lijn gebracht met landelijk beleid en richtlijnen informatiebeveiliging onder regie CISO

Distributie en geraadpleegde personen

Versie	Verzend datum	Naam, afdeling en functie
0.1.0	06-05-2015	5.1.2.e (5.1.2.e Implementatie Autorisatiemodel); 5.1.2.e (5.1.2.e ICT); 5.1.2.e (5.1.2.e Implementatie Autorisatiemodel); 5.1.2.e (5.1.2.e Functioneel Beheer); 5.1.2.e (5.1.2.e ICT); 5.1.2.e (Adviseur strategie); 5.1.2.e, 5.1.2.e (5.1.2.e beleid en implementatie); 5.1.2.e (juridisch adviseur); 5.1.2.e (beleidsadviseur GA) en 5.1.2.e (CISO)
0.2.0	01-06-2015	Idem als bij versie 01.0 alsmede 5.1.2.e, 5.1.2.e, 5.1.2.e (IM adviseurs); 5.1.2.e (IBF); 5.1.2.e (GGB)
0.2.1	05-06-2015	5.1.2.e (5.1.2.e Implementatie Autorisatiemodel); 5.1.2.e, 5.1.2.e, 5.1.2.e (project adviseurs)
0.2.1	26-06-2015	Stuurgroep autorisatiemodel politie: bespreekstuk
0.3	07-09-2015	Stuurgroep BI: bespreekstuk
0.3	08-10-2015	5.1.2.e (GA), 5.1.2.e (CISO)
0.4	02-11-2015	5.1.2.e (CISO)
0.5	19-11-2015	Projectleiding implementatie autorisatiemodel, projectgroep leden, GA en CISO
0.6	15-12-2015	Projectleiding implementatie autorisatiemodel, projectgroep leden, GA en CISO alsmede de leden van de stuurgroep autorisatiemodel politie
1.0	27-01-2016	MT-CIO, projectleiding implementatie autorisatiemodel, projectgroep leden, GA en CISO alsmede de leden van de stuurgroep autorisatiemodel politie

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
IV	Informatie Voorziening
IM	Informatie Management
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.

Aandachts-gebied	Een verbijzondering van een werkterrein, dat wordt gekenmerkt door een grote verscheidenheid aan onderwerpen, waardoor een specifieke inzet en inbreng geldt. Voor deze inzet kunnen nadere opleiding- en certificeringeisen worden gesteld.
Audit Based Access	Houdt in dat alleen achteraf bekeken wordt of gebruikers zich kunnen verantwoorden voor toegang tot data.
Attribute Based Access Control	Houdt in dat er geen autorisaties aan een persoon worden gegeven op grond van identiteit, maar op basis van attributen van een identiteit. Er worden regels gemaakt met deze attributen die het toegangsbeleid van de organisatie vertegenwoordigen.
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	Letterlijk: toepassing, is een computerprogramma dat bedoeld is voor eindgebruikers.
Attributen	Een eigenschap of kenmerk zoals die in een bestand wordt opgeslagen, bijvoorbeeld ‘functie’.
Autoriseren	Het machtigen van een persoon voor het verrichten van verwerkingshandelingen met gegevens.
Autorisatie- matrix	Het overzicht waarin alle actuele autorisatiematrixrollen in relatie zijn gebracht met toegestane gegevens verwerkingshandelingen.
Autorisatie- matrixrol	De rolbenaming ten behoeve van autorisaties die is gebaseerd op de combinatie van de toegekende LFNP functie, de feitelijke organisatie eenheid en het vakgebied.
Autorisatiemutatie	Iedere handmatige- of geautomatiseerde handeling, die inhoudelijk een verandering te weeg brengt in de bestaande gegevens, die betrekking heeft op autorisatie.
Autorisatie- profiel	De beschrijving van alle verwerkingsrechten die bij één of meerdere autorisatiematrixrollen behoort.
Autorisatie systeem (stelsel van autorisaties)	Het systeem 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 structureel actueel houden, onderhouden en wijzigen van de autorisatiematrixrollen en de autorisatiematrix.

Dynamische provisioning	Het systeem van automatisch en autonoom toekennen en verwijderen van permissies en autorisaties zonder menselijk inbreng gebaseerd op vooraf opgegeven waarden.
Gegevens	Die gegevens die in het kader van de uitvoering van een taak noodzakelijk kunnen zijn. Het kan hierbij gaan om politiegegevens en/of bedrijfsvoering gegevens.
Identificatie	Een methode, procedure en/of handeling om je ervan te verzekeren, dat iemand is, die hij/zij beweert te zijn.
Identity Management	Een geheel aan beleid, verantwoordelijkheden, processen en hulpmiddelen dat organisaties in staat stelt om van actoren (als gebruikers en systemen) de identificatie en authenticatie te faciliteren, beheren en controleren.
LFNP functie	De functiebenaming zoals die voorkomt in het Landelijk Functiehuis Nationale Politie. Hierbij zijn voor elke functie vastgelegd welke verantwoordelijkheden, taken, activiteiten en bevoegdheden, welke mate van zelfstandig handelen en welk werk- en denkniveau aan de functie verbonden zijn om deze naar behoren te kunnen invullen.
Leidinggevende	Medewerker, die leiding geeft aan een organisatieonderdeel waarin de politietaak wordt uitgevoerd of leiding geeft aan een organisatieonderdeel waar ondersteunende werkzaamheden aan deze politietaak uitgevoerd worden.
Mandateren/ delegeren	Mandaat is de bevoegdheid om in naam van een ander te handelen, maar zonder de daarbij horende verantwoordelijkheid. Bij mandateren worden geen bevoegdheden overgedragen. De mandaatgever blijft zelf bevoegd. Dit in tegenstelling tot delegeren, wat wel het overdragen van bevoegdheden betekent, inclusief de verantwoordelijkheid. Een mandaatgever blijft bevoegd de gemandateerde bevoegdheid zelf te hanteren.
Mutatiegegeven	Gegeven met een hoge wijzigingsfrequentie zoals ‘verwerkingsdatum’
Organisatie eenheid	De formatieve en/of feitelijke plaats in de organisatie waar taken en werkzaamheden worden uitgevoerd.
Permissie	Functionele afbeelding in het IAM van een ‘applicatierol’ in het doelsysteem.
Primaire opleidingseisen	Die opleidingseisen die genoemd zijn in een LFNP functieprofiel.
Provisioning	Het deelproces binnen het Identity & Access Management proces waarmee aan een individu autorisaties voor informatiesystemen of computersystemen worden verstrekt. Daarbij worden de rechten verstrekt op basis van de functie en rol van de persoon binnen een automatiseringsomgeving.

Rol	Een verzameling permissies, benodigd om de rol te kunnen vervullen.
Role Based Access Control	Toegang wordt automatisch bepaald op basis van de rol van een gebruiker binnen een bedrijfsproces.
Secundaire opleidingseisen	Die opleidingseisen die gekoppeld zijn aan een vakgebied en of additionele taken.
Stamgegevens	Vaste of referentie gegevens. Stamgegeven kennen een (zeer) geringe wijzigingsfrequentie in tegenstelling tot muterende gegevens zoals ‘geboortedatum’.
Specifieke functionaliteit	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-voorwaarden	Die voorwaarden waaraan voldaan moet worden om toegang tot gegevens te verkrijgen.
Vakgebied	De verzameling van specifieke taken die binnen een LFNP functie ten behoeve van een organisatie eenheid worden uitgevoerd. Een clustering van in essentie gelijkgerichte activiteiten, en beoogde effecten op basis van voor dat vakgebied geldende processen.
Werkterrein	Een verbijzondering van het vakgebied, waarvoor een specifieke inzet en inbreng geldt. Voor deze inzet kunnen nadere opleiding- en certificeringseisen worden gesteld.

Inhoudsopgave

1. Inleiding

Een politiemedewerker is een professional die op een juiste wijze omgaat met de gegevens die hij/zij beschikbaar gesteld krijgt om zijn taak te kunnen uitvoeren.

De medewerkers moeten zoveel als mogelijk gegevens delen met die collega's die deze gegevens ook nodig hebben voor hun werk. Zij moeten dit doen op basis van een systeem van autorisaties, dat gebaseerd is op vertrouwen in elkaars professionaliteit. Zij moeten toegang kunnen krijgen tot de gegevens die zij nodig hebben voor hun werk en daar verantwoording over (kunnen) afleggen.

De korpschef is verantwoordelijk voor het onderhouden van 'een systeem van autorisaties' dat voldoet aan 'de vereisten van zorgvuldigheid en evenredigheid'. Binnen de directie IV is de functie van de CISO ingericht voor toezicht op het stelsel van autoriseren vanuit de bredere rol voor informatiebeveiliging.

Het beleid voor de vernieuwing van de autorisatiesystematiek levert een bijdrage aan de effectiviteit van de politieorganisatie en biedt waarborgen tegen het onjuist gebruik van autorisaties.

Door op een zoveel mogelijk geautomatiseerde manier van autorisatiebeheer, binnen de kaders van de wet, op basis van het 'delen tenzij de wet dat niet toestaat' beginsel voor gegevens, wordt daarnaast bijgedragen aan een effectievere uitvoeringsorganisatie en een efficiënter omgang met de beheerkosten.

Het beleid draagt bij aan de borging van de kwaliteit van verkrijging, verwerking en gebruik van politiegegevens en bedrijfsvoeringgegevens.

Daarnaast draagt het beleid bij aan de borging van het veilig verwerken van gegevens binnen het beleid voor informatiebeveiliging.

2. Voorgeschiedenis: op weg naar nieuwe kaders

De Korpschef is expliciet verantwoordelijk voor het onderhouden van een systeem van autorisaties dat voldoet aan de vereisten van zorgvuldigheid en evenredigheid.
In het hierna volgende wordt ingegaan op de ontwikkelingen die hebben geleid tot de huidige stand van zaken.

In juli 2011 is door de toenmalige Raad van Korpschefs de visie op een landelijk autorisatiemodel “Autoriseren: zo doen we dat hier!” vastgesteld. Hierin is het “delen, tenzij de wet dat niet toestaat” principe voor de politieorganisatie vastgelegd, maar specifiek binnen de kaders van de Wpg.

Bij de verdere inrichting van het autorisatiebeheer is dit principe als basis blijven dienen. In bijlage 1 is het model opgenomen waarin deze visie is geconcretiseerd voor autorisaties voor de uitvoering van de politietaak. Kernpunten uit de visie zijn:

- ‘delen van gegevens tenzij de wet dat niet toestaat’ en delen ‘by the book’ waarbij een evenwicht tussen informatie delen en het voorkomen van afbreukrisico’s;
- professionaliteit van en vertrouwen in medewerkers staan centraal;
- de combinatie LFNP functie, werkzaamheden en organisatorische plaats geven op rollen gebaseerde autorisaties, waarbij de autorisatieprofielen voor dezelfde ‘combinatie’ landelijk gelijk zijn;
- toegang tot informatie is in principe landelijk, de fysieke werklocatie is daarbij niet relevant;
- ten aanzien van autorisaties wordt een eenduidig, landelijk, eenvoudig en transparant proces gehanteerd;
- daar waar dat mogelijk is worden toe te kennen permissies geautomatiseerd opgeleverd;
- toegang tot gegevens wordt verleend op basis van noodzakelijkheid.

De politie streeft naar één landelijke informatievoorziening. Bij de inrichting van de nieuwe informatievoorziening staat het werk van de politiecollega’s centraal en daarnaast de benodigde uniformering van ICT-voorzieningen. De nieuwe waarden van de NP zijn georganiseerd vertrouwen en medewerkersparticipatie.

In 2014 is onder andere op basis van de wens om over een meer flexibele organisatie-inrichting te komen gestart met het herzien van het systeem van autorisaties aan de hand van de eerdergenoemde visie ‘Autoriseren; zo doen we dat hier’.

Eveneens in 2014 is begonnen met het projectmatig realiseren van Identity en Access Management (IAM) onder verantwoordelijkheid van de stuurgroep Business Intelligence.

In 2015 zijn de eerste concrete stappen gezet, op weg naar nieuwe kaders en een nieuwe dynamiek waarin het systeem van autorisaties moet functioneren. De IAM tool is in werking gegaan. Gewezen wordt op het feit dat niet alle onderwerpen van dit autorisatiebeleid in het project IAM gerealiseerd worden. De scope van het project is genoemd in de bijbehorende PID en faseplannen van het project Implementatie Autorisatiemodel Politie.

3. Afbakening

De politie is verantwoordelijk voor iedereen aan wie zij een autorisatie geeft en voor iedere toegang tot informatie die zij in beheer heeft. Dus:

1. Autorisaties voor alle medewerkers en externen voor toegang tot systemen waarvoor de politie een beheerverantwoordelijkheid draagt;
2. Autorisaties die de politie in opdracht van een ander geeft voor de toegang tot gegevens in systemen van die ander;
3. Autorisaties die derden krijgen voor toegang tot gegevens van bij de politie in beheer zijnde systemen/informatie

Het gaat niet uitsluitend over de applicaties voor de politietaak en politiegegevens, maar om alle gegevens die binnen een systeem worden verwerkt door de politie, ongeacht of het voor de politietaak (Wpg regiem) of voor de bedrijfsvoering (Wbp regiem) is.

Gegevens in eigendom van andere partijen dan de politie blijven buiten beschouwing tenzij in een wettelijke regeling of rechtsgeldig convenant is bepaald dat de politie daartoe rechtstreeks toegang moet kunnen krijgen. In dat laatste geval moet ook de toegang tot deze gegevens worden geregeld.

Partners (externe partijen) die op grond van een wettelijke regeling of een rechtsgeldig convenant toegang krijgen tot gegevens van de politie vallen binnen de werking van het beleid.

Het verstrekken van politie-informatie is geen onderdeel van het beleid.

Beleid ten aanzien van de autorisaties voor fysieke toegang tot gebouwen, terreinen, speciale ruimtes en specifieke middelen, blijft buiten beschouwing.

4. Uitgangspunten

Het belangrijkste uitgangspunt is dat dat men binnen het politieveld de politiegegevens aan elkaar beschikbaar moet stellen, tenzij het de goede uitvoering van de politietaak niet dient of wettelijk niet is toegestaan.

Een ander belangrijk uitgangspunt is dat de organisatie waar het gaat om autorisatiebeheer snel en adequaat moet kunnen reageren op maatschappelijke ontwikkelingen, incidenten en op elke verandering in de positie van elke medewerker.

Het autorisatiebeleid is van toepassing op zowel politiegegevens (regiem Wpg) als bedrijfsvoeringgegevens (regiem Wbp).

5. Doelen

De reikwijdte van de autorisaties moet recht doen aan de noodzaak om tot een efficiënte en effectieve uitvoering en de ondersteuning van de politietaak te kunnen komen. Ook moet het recht blijven doen aan de belangen die gediend worden met de nakoming van de normen voor privacybescherming, voor informatieveiligheid van de gegevens en de verwerking ervan.

In de kern wordt met het thans voorgestelde beleid voor de komende vijf jaar het volgende nagestreefd.

Van applicatie naar gegevens

Er is zoveel als mogelijk een naadloze overgang tot stand gebracht van het actuele systeem van geautomatiseerde toekenning op basis van applicaties, naar een nieuw stelsel van geautomatiseerde toekenningen op basis van gegevens.

Rechtmatig / voldoet aan de Wpg en Wbp

De grenzen van de vigerende wet- en regelgeving worden door de reikwijdte van de geautomatiseerde toegekende autorisaties van het nieuwe stelsel van geautomatiseerde toekenningen van autorisaties niet overschrijden. Er wordt voldaan aan de vereisten van zorgvuldigheid en evenredigheid[1]. In de bijlage is een nadere uitwerking gegeven aan de elementen die in acht moeten worden genomen bij het uitwerken van een autorisatiesysteem dat voldoet aan de vereisten van zorgvuldigheid en evenredigheid.

Medewerkers en informatiegedrag

De geautoriseerde kent zijn/haar verantwoordelijkheid. Hij/zij kan beoordelen of hij/zij zich gedraagt conform de eisen die door de politie worden gesteld aan het gehanteerde systeem van autorisaties voor de politie.

Bewust van brede toegang, maar beperkt gebruik

Voor zover een permissie toestaat dat een medewerker over meer gegevens kan beschikken dan nodig is voor de uitvoering van de eigen taak, is deze zich ervan bewust dat hij/zij dan uitsluitend gebruik maakt van die gegevens die hij/zij feitelijk zelf nodig heeft voor de aan hem/haar opgedragen taak.

Delen, tenzij de wet dat niet toestaat

De medewerker stelt de gegevens die hij/zij vastlegt, in principe beschikbaar aan de collega's die deze gegevens eveneens behoeven voor de aan hen opgedragen taak, tenzij wet- of regelgeving en interne richtlijnen zich daartegen verzetten.

Landelijk eenduidig, uniform en transparant

Het nieuwe stelsel van geautomatiseerde toekenning van toegang tot gegevens wordt over het gehele land in de organisatieonderdelen eenduidig, uniform en transparant uitgevoerd.

[1] Onder andere artikel 6.1 Wpg

Voor externe partners geldt hetzelfde

Door de positie die de politie in de maatschappij inneemt fungeert de organisatie als intermediair binnen vele vraagstukken, doelgroepen en dient ze vele maatschappelijke belangen. Het is dan ook een logisch gevolg dat de politie, gegevens deelt met de daarvoor bestemde doelgroepen binnen dezelfde kaders.

Beheersbaar en beheerbaar

De processen rond de uitvoering van het autoriseren zijn zodanig ingericht dat optimaal tegemoet wordt gekomen aan de landelijke eenduidige, uniforme en transparante invoering en uitvoering van de geautomatiseerde autorisatietoekenning. Administratieve handelingen zijn tot het noodzakelijke minimum teruggebracht. Het aantal autorisatiematrixrollen is beheerbaar en tot het praktisch haalbare minimum beperkt.

Borgen van de reikwijdte van autorisaties

Voor de gegevens waarvoor men geautoriseerd wordt, is geborgd dat er zo snel mogelijk gecorrigeerd wordt wanneer:

- het gebruik van de gegevens niet kan worden verantwoord;
- deze voor een ander doel worden gebruikt dan waarvoor die gegevens verkregen zijn (doelbinding);
- het gebruik niet in verhouding staat tot wat er mee beoogd wordt (proportionaliteit);
- indien het doel, waarvoor de gegevens toegankelijk zijn gemaakt, kan worden bereikt op een wijze die minder ingrijpend (proportionaliteit) dan wel minder bezwaarlijk is voor de burger (subsidiariteit) vanuit oogpunt van privacybescherming;
- deze niet op een passende wijze zijn beveiligd tegen onbedoelde of onrechtmatige toegang ertoe en ongewenste verwerking, verwijdering, vernietiging of bekendmaking ervan;
- deze niet zijn verwijderd of worden vernietigd wanneer zijn niet langer noodzakelijk zijn voor het doel waarvoor ze zijn verwerkt dan wel wanneer dit door wettelijke bepalingen wordt vereist (bewaartermijnen van Wpg en Wbp).

In lijn met wat geleerd is van best practices

Stelsel van maatregelen voor het beheren van de autorisaties zijn mede gebaseerd op datgene wat elders bij andere grote organisaties als leerpunten is verzameld en aldus zo veel als mogelijk in lijn werkt met de best bewezen praktijk.

Toegang voor beheer

De medewerkers belast met het beheer van de geautomatiseerde informatiesystemen, hebben toegang tot de systemen en applicaties die zij in beheer nemen, echter alleen voor zover dat vereist is voor de hen toekomende beheeropdracht (least priveleged principle).

Dekkingsgraad zo hoog als mogelijk

De geautomatiseerde toegang verlening tot gegevens dekt het politiewerk zo veel als mogelijk toe wat behoeft wordt voor de opgedragen taak. Dit in evenwicht tussen beheersbaarheid van het geautomatiseerde stelsel en het handmatig toekennen van uitzonderingen. Er zullen altijd medewerkers zijn die zodanig specialistische taken uitvoeren dat deze niet of niet meteen in deze context passen. Voor hen zal er een daartoe noodzakelijke constructie bestaan die zoveel

mogelijk aansluit op het systeem van toekennen van autorisaties en van het toezicht en de controle op het stelsel van autorisaties.

Informatiebeveiliging

Het actuele Informatiebeveiligingsbeleid en -kader Politie is leidend waar het gaat om het effectueren van informatiebeveiliging in samenhang met het systeem van autorisaties. Het volgende is daartoe geëffectueerd:

- leidinggevenden nemen hun verantwoordelijkheid in het stimuleren en uitdragen van veilig gedrag aangaande het gebruik van de toegekende autorisaties;
- de medewerkers gaan verantwoordelijk om met gegevens, ondersteund door beveiligingsinstructies en technische maatregelen;
- verantwoordelijkheden en bevoegdheden in het autorisatieproces, zijn mede met het oog op IT-beveiliging vastgelegd binnen alle niveaus van de organisatie, en elke medewerker is op de hoogte wat dit voor de betreffende functie inhoudt en handelt hiernaar;
- de regels voor toegang tot en gebruik van informatie, systemen en bedrijfsmiddelen zijn bekend bij de medewerkers;
- de regels voor een veilige informatie-uitwisseling, ook in de keten, zijn bekend bij de medewerkers;
- functiescheiding wordt aangehouden teneinde misbruik van de processen en informatie te voorkomen.

Gegevensbeheer

Het actuele beleidskader voor de GA is leidend waar het gaat om het effectueren van de verbetering van kwaliteit uitwisseling van gegevens in samenhang met het systeem van autorisaties. De medewerker zet de gegevens maximaal in voor betere politieprestaties, voor meer legitimiteit en groter vertrouwen in de politie en voor het functioneren als één korps.

Bevoegdheid kent grenzen

De medewerker heeft de vrijheid om, met inachtneming van de professionele standaarden, gebruik te maken van de gegevens waartoe deze toegang krijgt. Echter in geval van oneigenlijk gebruik of van misbruik van beschikbaar gekomen gegevens wordt dit beschouwd als een handeling die ernstig afbreuk doet aan de instandhouding van het stelsel van autorisaties en aan het in de medewerker gestelde vertrouwen. De naleving van de regels en normen (landelijke gedragscode) van Veiligheid, Integriteit en Klachten zijn aan de orde.

Evaluatie

Regelmatig dan wel op enig moment op aanwijzing moet beoordeeld kunnen worden of de toegekende autorisaties nog voldoen aan het vereiste van ‘nodig om de taak te kunnen uitoefenen’. Regelmatig wordt het autorisatiesysteem als geheel geëvalueerd.

6. Randvoorwaarden

De basisrandvoorwaarde voor het autoriseren van medewerkers van de politie en van partners is dat sprake is geweest van het op de juiste wijze toekennen van functies met inachtneming van eventuele aan de functies gekoppelde screenings- en opleidingseisen.

Daarnaast gelden de volgende randvoorwaarden.

Eigenaarschap autorisatiebeheerproces

De CIO is binnen de KL portefeuillehouder voor informatiebeveiliging (inclusief autoriseren), de CISO is als eigenaar van het autorisatiebeheerproces benoemd. Deze is gemandateerd om finale beslissingen te nemen over wijzigingsvoorstellen met betrekking tot het autorisatiebeheerproces.

Bewustwording en adequate opleiding

De politieorganisatie biedt adequate mogelijkheden gericht op het bewust worden op de eigen verantwoordelijk van elke medewerker voor de haar/hem toegekende toegangs- en verwerkingsrechten van gegevens en rekening houdend met de verantwoordelijkheid van de leidinggevende. Dit betekent dat hij/zij kan weten:

- hoe de gegevenshuishouding binnen de Nationale Politie is georganiseerd en ingericht;
- welke relevante gegevens waar en wanneer voor hem/haar beschikbaar zijn;
- binnen welke kaders en normen van informatiebeveiliging, van gegevensverwerking en van integriteitseisen hij/zij zich behoort te gedragen bij het gebruik maken van zijn/haar autorisaties.

Rubricering van gegevens

Er is een actuele en goedgekeurde regeling voor rubricering van gegevens. Dit helpt mede te bepalen welke autorisaties de medewerker geautomatiseerd toebedeeld kan krijgen in relatie tot zijn/haar taakuitoefening binnen de politieoperatie.

Eisen voor risicobeheersing

De KL levert de eisen aan op grond waarvan het voldoende moet worden geacht dat de risico's van onjuist gebruik of misbruik tot een aanvaardbaar minimum zijn gebracht.

HR proces en systeem

HR levert de procedures die gevolgd moeten worden voor de in-, door- en uitstroom van medewerkers, die de voeding vormen voor een leidend HR-systeem (thans Beaufort NP). Op basis van dit leidende HR systeem worden op basis van de combinatie LFNP functie, organisatorische plaats en toegewezen vakgebied, de geautomatiseerde toekenning, actualisatie en verwijdering van autorisaties doorgevoerd.

Partners

Voor de partners van de politie stelt de eigenaar van het autorisatiebeheerproces de reikwijdte en organisatorische afspraken vast ten aanzien van de eventueel toe te kennen autorisaties voor toegang tot gegevens van de politie.

Inrichting IT infrastructuur

De IT-infrastructuur wordt ingericht op de eisen die het vanuit het stelsel van informatiebeveiliging worden gesteld aan onder meer beschikbaarheid van gegevens, performance, robuustheid en schaalbaarheid.

Randvoorwaarden gesteld door OM

Het OM stelt randvoorwaarden[2] aan het systeem van autorisaties met betrekking tot de verwerking van politiegegevens binnen TCI (art. 10 Wpg). Deze randvoorwaarden worden gevolgd met het oog op verwerking van 'deelbare' en 'voor intel use only' politiegegevens.

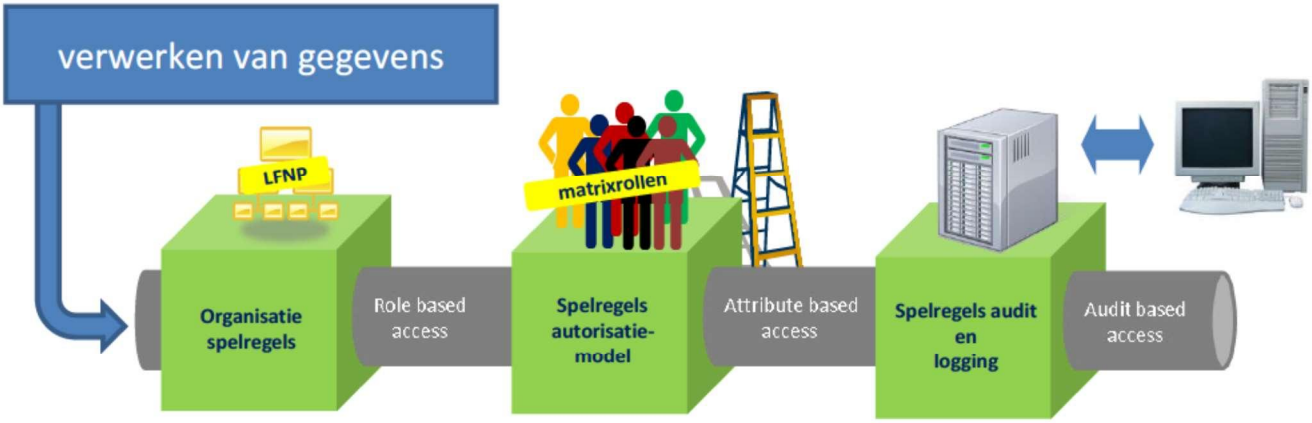
[2] brief van 23 oktober 2014 (Pa/BGS/17115)

Bijlage 1 Visie “Autoriseren: zo doen we dat hier!”

In de kern bevat de visie het volgende autorisatiemodel:

5.1.2.i

Bijlage 2 Samenvattend overzicht access vormen



Role Based Access Control (RBAC), Attribute Access Control (ABAC) en Audit Based Access Control (ABA) zijn aan elkaar ondersteunende processen die gezamenlijk de borging van controle en toezicht op het systeem van autorisaties van de politie vorm geven. Dit komt overeen met de thans gangbare werkwijze (best practice) die breed binnen grote organisaties, met oog op het verantwoord autoriseren, in het bedrijfsleven is geïmplementeerd en bewezen succesvol wordt gehanteerd.

Toelichting op Role Based Access Control (RBAC)

Individuen worden niet rechtstreeks geautoriseerd in informatiesystemen, Zij krijgen uitsluitend rechten door een vorm van groepslidmaatschap, op basis van de rol die ze hebben binnen een organisatie of bedrijfsproces. Ook de permissies op objecten/functies in informatiesystemen kunnen worden gegroepeerd in rollen. De inhoud van de autorisatiematrixrol wordt vooraf goedgekeurd door of namens de korpsleiding.
Door het koppelen van de rol van de gebruiker in de organisatie aan een rol in een informatiesysteem, is het eenvoudig om de effectieve rechten van een gebruiker te bepalen. Het daadwerkelijk geautomatiseerd toekennen van rechten en permissies aan een gebruiker is provisioning.

Toelichting Attribute Based Access Control (ABAC)

Er worden geen autorisaties aan een persoon gegeven op grond van identiteit, maar op basis van attributen van een identiteit. Er worden regels gemaakt met deze attributen die het toegangsbeleid van de organisatie vertegenwoordigen. Voorbeeld attributen zijn: functie, doelgroep, adresgegevens of werkplek, locatie, tijd-, lees-, schrijf- en uitvoerrechten. Het voordeel hiervan is het kunnen reguleren van real-time toegang tot alle informatie binnen een organisatie, voor elke type aanvraag. en grootschalig administratief model niet nodig.

Toelichting op Audit Based Access Control (ABA)

Met de ruimere toegang tot gegevens kan oneigenlijk gebruik van deze gegevens niet worden uitgesloten. Zodanig moet er ter ondersteuning van ABA een goed controle (audit) proces en sanctiebeleid zijn, de kans op controle en een eventuele sanctie achteraf moet misbruik

voldoende gesanctioneerd kunnen worden. Herleidbaarheid van de gebruiker en de acties van deze gebruiker moeten dan ook altijd te achterhalen zijn wil ABA succesvol zijn. De focus van ABA concentreert zich volledig op de vraag of de medewerker de verwerking heeft verricht binnen de hem daarvoor opgelegde taakstelling.

Omdat er in de visie op autoriseren autorisaties breed worden toebedeeld is het van belang dat de gebruiker correct wordt geïnstrueerd en opgeleid in de wijziging van het autorisatiebeleid. Meerdere rechten die binnen de (politie)taakstelling vallen hoeven niet altijd daadwerkelijk voor de gebruiker van toepassing te zijn. Ruimere autorisaties versnelt het delen van informatie binnen de organisatie. De controle achteraf moet aantonen of het gebruik ervan rechtmatig is geweest. In het beleid wordt de voorkeur gegeven aan het monitoren op excepties en ‘need to access’.

Er wordt alleen achteraf bekeken of gebruikers zich kunnen verantwoorden voor toegang tot data. Controlerende functionarissen of één of meer auditors kunnen een gebruiker om verantwoording vragen. Om deze stap binnen het proces mogelijk te maken wordt voor de controle- of auditfunctie een lijst bijgehouden welke gebruikers welke data hebben opgevraagd (Audit Trail).