INFORMATIE
BEVEILIGINGS
DIENST

BELEID LOGISCHE TOEGANGSBEVEILIGING

Een van de producten van de operationele variant van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG)

KWALITEITSINSTITUUT NEDERLANDSE GEMEENTEN IN OPDRACHT VAN
VERENIGING VAN NEDERLANDSE GEMEENTEN

INFORMATIE
BEVEILIGINGS
DIENST

Colofon

Naam document
Beleid logische toegangsbeveiliging

Versienummer
1.0

Versiedatum
Juli 2014

Versiebeheer
Het beheer van dit document berust bij de Informatiebeveiligingsdienst voor gemeenten (IBD).

Met dank aan
De expertgroep en de reviewgemeenten die hebben bijgedragen aan het vervaardigen van dit product.

In samenwerking met
De producten van de operationele variant van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) worden vervaardigd in samenwerking met:

KWALITEITSINSTITUUT NEDERLANDSE GEMEENTEN IN OPDRACHT VAN VERENIGING VAN NEDERLANDSE GEMEENTEN

INFORMATIE
BEVEILIGINGS
DIENST

Voorwoord

De IBD is een gezamenlijk initiatief van de Vereniging van Nederlandse Gemeenten (VNG) en het Kwaliteitsinstituut Nederlandse Gemeenten (KING) en actief sinds 1 januari 2013. Aanleiding voor de oprichting van de IBD vormen enerzijds de leerpunten uit een aantal grote incidenten op informatiebeveiligingsvlak en anderzijds de visie Digitale Overheid 2017.
De IBD is er voor alle gemeenten en richt zich op bewustwording en concrete ondersteuning om gemeenten te helpen hun informatiebeveiliging naar een hoger plan te tillen.

De IBD heeft drie doelen:

1. Het preventief en structureel ondersteunen van gemeenten bij het opbouwen en onderhouden van bewustzijn als het gaat om informatiebeveiliging.
2. Het leveren van integrale coördinatie en concrete ondersteuning op gemeente specifieke aspecten in geval van incidenten en crisissituaties op het vlak van informatiebeveiliging.
3. Het bieden van gerichte projectmatige ondersteuning op deelgebieden om informatiebeveiliging in de praktijk van alle dag naar een hoger plan te tillen. De ondersteuning die de IBD biedt bij het ICT-Beveiligingsassessment DigiD is een voorbeeld van zo'n project.

Hoe realiseert de IBD haar doelen?

Om invulling te kunnen geven aan haar doelen is door de IBD op basis van de Baseline Informatiebeveiliging Rijksdienst (BIR) een vertaalslag gemaakt naar een baseline voor de gemeentelijke markt. Deze Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) betreft twee varianten, een Strategische- én een Tactische Baseline. Beide varianten van de BIG zijn beschikbaar voor alle gemeenten op de website en community van de IBD, zodat door iedere gemeente tot implementatie van de BIG kan worden overgegaan. Bestuur en management hebben met deze baseline een instrument in handen waarmee zij in staat zijn om te meten of de organisatie 'in control' is op het gebied van informatiebeveiliging. Om de implementatie van de Strategische- en Tactische Baseline te ondersteunen, zijn door de IBD in samenwerking met de Taskforce Bestuur en Informatieveiligheid Dienstverlening (Taskforce BID) producten ontwikkeld op operationeel niveau. Dit heeft een productenportfolio opgeleverd, genaamd de Operationele Baseline Nederlandse Gemeenten (Operationele BIG). Onderhavig product is er één van.
Naast een productenportfolio, heeft de IBD voor gemeenten ook een dienstenportfolio ontwikkeld. Voor een volledig overzicht van het producten- en dienstenportfolio, kunt u terecht op de website van de IBD.

De gemeente is zelf verantwoordelijk voor het opstellen en/of uitvoeren en/of handhaven van de regels. Hierbij geldt:

- Er is wetgeving waar altijd aan voldaan moet worden, zoals niet uitputtend: BRP, SUWI, BAG en PUN, maar ook de archiefwet.
- Er is een gemeenschappelijk normenkader als basis: de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG).
- De gemeente stelt dit normenkader vast, waarbij er ruimte is in de naleving van dat kader voor afweging en prioritering op basis van het 'pas toe of leg uit' principe.

KWALITEITSINSTITUUT NEDERLANDSE GEMEENTEN IN OPDRACHT VAN VERENIGING VAN NEDERLANDSE GEMEENTEN

Leeswijzer

Dit product maakt onderdeel uit van de operationele variant van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG).

Doel
Dit product bevat aanwijzingen en een beleid rondom het inrichten van logische toegangsbeveiliging binnen de gemeente.

Doelgroep
Dit document is van belang voor medewerkers binnen de gemeente die verantwoordelijk zijn voor logische toegangsbeveiliging en de eindgebruikers.

Relatie met overige producten

- Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG)
  - Strategische Baseline Informatiebeveiliging Nederlandse Gemeenten
  - Tactische Baseline Informatiebeveiliging Nederlandse Gemeenten
- Het voorbeeld Informatiebeveiligingsbeleid van de gemeente, §6.1 en §7.1

Maatregelen tactische variant Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG).

Maatregel 10.1.3	Functiescheiding
Maatregel 10.10.2	Controle van systeemgebruik
Maatregel 11.1	Toegangsbeleid
Maatregel 11.2	Beheer van toegangsrechten van gebruikers
Maatregel 11.3.3	Clear desk en clear screen
Maatregel 11.4.6	Beheersmaatregelen voor netwerkverbindingen
Maatregel 11.4.7	Beheersmaatregelen voor netwerkroutering
Maatregel 11.5.1	Beveiligde inlogprocedures
Maatregel 11.5.2	Gebruikers identificatie en authenticatie
Maatregel 11.5.5	Time-out van sessies
Maatregel 11.5.6	Beperking van verbindingstijd
Maatregel 11.6.1	Beperken van toegang tot informatie

KWALITEITSINSTITUUT NEDERLANDSE GEMEENTEN IN OPDRACHT VAN VERENIGING VAN NEDERLANDSE GEMEENTEN

Inhoud

KWALITEITSINSTITUUT NEDERLANDSE GEMEENTEN IN OPDRACHT VAN
VERENIGING VAN NEDERLANDSE GEMEENTEN

1 Inleiding

Ten behoeve van de beveiliging van gemeentelijke informatiesystemen en de informatie binnen deze gemeentelijke informatiesystemen is dit beleid er op gericht hoe met logische toegangsbeveiliging omgegaan moet worden.

In de BIG worden eisen benoemd met betrekking tot logische toegangsbeveiliging en daarnaast staan in hoofdstuk 7 van het voorbeeld Informatiebeveiligingsbeleid van de gemeente, beheersmaatregelen in relatie tot logische toegangsbeveiliging. Dit document geeft algemene aanwijzingen over het inrichten van logische toegangsbeveiliging. Als laatste is er aanvullend een voorbeeld gemeentelijk beleid logische toegangsbeveiliging en een voorbeeld autorisatieprocedure.

1.1 Het belang van logische toegangsbeveiliging

Logische toegangsbeveiliging vormt een belangrijk aspect van de gemeentelijke informatiebeveiliging. Logische toegangsbeveiliging zorgt ervoor dat onbevoegden minder makkelijk toegang kunnen krijgen tot gemeentelijke informatiesystemen en de informatie binnen deze gemeentelijke informatiesystemen. Het kan hierbij ook gaan om bedrijfsinformatie van derde partijen, waarvan de gemeente niet de bronhouder is, indien deze via het gemeentelijk platform ontsloten en beschikbaar gesteld wordt, bijvoorbeeld Basisregistratie Personen (BRP)[1] en Suwinet[2]. Alle gebruikers van gemeentelijke informatiesystemen dienen, volgens logische toegangsbeveiliging procedures, geautoriseerd te worden.

Risico's

Door het ontbreken van adequate logische toegangsbeveiliging bestaat het risico dat onbevoegden zich toegang kunnen verschaffen tot gemeentelijke informatiesystemen en de informatie binnen deze gemeentelijke informatiesystemen, waardoor ongewenste acties op de diensten kunnen plaatsvinden en/of informatie kan worden ontvreemd of verminkt.
Onduidelijke of niet gevolgde logische toegangsbeveiliging procedures zijn niet alleen een bedreiging voor de vertrouwelijkheid en integriteit van gemeentelijke informatie, maar uiteindelijk ook slecht voor het imago van de gemeente.[3]

1.2 Raakvlakken

Overige raakvlakken die logische toegangsbeveiliging hebben met de BIG zijn:

- Dataclassificatie (classificatie van bedrijfsmiddelen en informatie)
- Geheimhoudingsverklaringen
- ICT-beheer (oplevering, acceptatie en overdracht van (delen van) systemen, beheerorganisatie en beheerprocessen)
- Informatiebeveiligingsbeleid van de gemeente
- Logging (controle, auditing en monitoring)
- Telewerken

[1] De Basisregistratie Personen (BRP) heeft de Gemeentelijke Basisadministratie Personen (GBA) vervangen.
[2] Suwinet is het informatiesysteem van gegevensuitwisseling op het terrein van werk en inkomen
[3] Zie hiervoor bijvoorbeeld 'Veilig gebruik Suwinet' (http://www.bkwi.nl/veiligheid/veilig-gebruik-suwinet/ en http://www.vng.nl/onderwerpenindex/sociale-zaken/samenwerken-op-de-arbeidsmarkt/nieuws/staatssecretaris-schrijft-gemeenten-aan-over-veilig-gebruik-van-suwinet). In 2013 onderzocht de Inspectie SZW hoe gemeenten omgaan met de informatiebeveiliging van Suwinet, er werd onder andere getoetst op de normen functiescheiding en autorisatiestructuur. Uit dit onderzoek bleek dat slechts drie gemeenten goed scoorden op de normen.

- Toegangsbeleid
- Wachtwoordbeleid

2 Logische toegangsbeveiliging

Informatie speelt een belangrijke rol in bedrijfsprocessen en hierdoor krijgt ook de beveiliging van de informatie een steeds hogere prioriteit. Om goed te kunnen functioneren is het voor de gemeente van belang dat zij tijdig over relevante en betrouwbare informatie beschikt. Om de informatiestromen te beheersen dient de gemeente een proces in te richten dat bepaalt wie er wanneer toegang heeft tot informatie. Logische toegang is gebaseerd op de classificatie van informatie.[4]

Definitie
Er worden diverse definities gehanteerd voor logische toegangsbeveiliging en in bijna alle definities staat het beheersen van toegang tot gegevens en informatiesystemen centraal. Daarom hanteren we de volgende definitie voor logische toegangsbeveiliging: 'Logische toegangsbeveiliging is het geheel aan maatregelen welke tot doel hebben, de toegang tot gegevens en informatiesystemen te beheersen zodat gegevens, informatiesystemen en resources worden beschermd tegen ongeautoriseerde acties'. Onder acties wordt onder andere verstaan: raadplegen, wijzigen en gebruik.

Doelstelling
Doelstelling van logische toegangsbeveiliging is het vaststellen van de identiteit[5] (authenticeren) van een gebruiker die toegang krijgt tot gemeentelijke gegevens, informatiesystemen of diensten,[6] en het waarborgen van een gecontroleerde toegang (autoriseren) tot, en gebruik van, gemeentelijke gegevens, informatiesystemen of diensten door gemeentemedewerkers, en/of een derde partij tegen acceptabele kosten.

Logische versus fysieke toegangsbeveiliging
Het fysieke en logische toegangsbeheer van organisaties wordt vaak nog gescheiden uitgevoerd. Maar integratie van fysieke en logische toegangsbeheer geeft een 'veiligere' en efficiëntere situatie. Fysiek toegangsbeheer[7] heeft betrekking op de toegang tot gebouwen, logisch toegangsbeheer heeft betrekking op de toegang tot informatiesystemen. Geconvergeerde toegangssystemen, waarin het fysieke en logische toegangsbeheer zijn geïntegreerd, gebruiken gegevens van zowel fysieke beveiliging als ICT-beveiliging. Een geconvergeerd systeem maakt de controle op, en het beheer van toegangsbeveiliging gemakkelijker. Bijvoorbeeld door het centraal toekennen en intrekken van bevoegdheden bij nieuw of vertrekkend personeel.

Uitgangspunten
Bij het ontwerpen en implementeren van logische toegangsbeveiliging dienen de volgende uitgangspunten gehanteerd te worden:

- De systeemeigenaar overlegt met de betrokken gegevenseigenaren en proceseigenaren over de vraag wie geautoriseerd wordt en op welke manier dat gebeurt.

[4] Zie hiervoor ook het operationele product 'Handreiking Dataclassificatie' van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG).
[5] Volgens De Van Dale Grote woordenboeken 2008 hedendaags Nederlands betekent identiteit; gelijkheid van naam en persoon. Bij logische toegangsbeveiliging kan het hierbij zowel over personen als systemen of diensten gaan. Deze worden alle aangeduid als gebruiker.
[6] Het kan hierbij ook gaan om bedrijfsinformatie van derde partijen, waarvan de gemeente niet de bronhouder is, indien deze via het gemeentelijk platform wordt ontsloten en beschikbaar gesteld wordt.
[7] Zie hiervoor ook het operationele product 'Toegangsbeleid' van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG).

- Er worden in de regel geen 'algemene' (ongepersonaliseerde) identiteiten gebruikt. Voor herleidbaarheid en transparantie is het namelijk nodig om te weten wie een bepaalde actie heeft uitgevoerd.
- De gemeente maakt, waar mogelijk, gebruik van bestaande (landelijke) voorzieningen voor authenticatie, autorisatie en informatiebeveiliging of heeft een eigen voorziening voor gebruikersbeheer. Voor burgers en bedrijfsleven gelden DigiD[8] en eHerkenning[9].

Beleid logische toegangsbeveiliging

Er is een door het management goedgekeurd beleid voor het beheer van de logische toegangsbeveiliging aanwezig. In dit beleid is aangegeven hoe logische toegangsbeveiliging is geregeld in de gemeente en dient de volgende onderwerpen te behandelen:

- **Gebruikersbeheer**: Is het proces dat gericht is op het aanvragen, wijzigen en verwijderen van gebruikers.
- **Toegangsbeheer**: Is het proces dat gericht is op het aanvragen, wijzigen en verwijderen van autorisaties.
- **Functiescheiding**: Functiescheiding is geregeld zodat afzonderlijke functionarissen zijn aangewezen die autorisaties aanvragen/toekennen, wijzigen, intrekken en/of verwijderen en controleren.

Bewustwording

Er dient door de gemeente specifiek aandacht geschonken te worden aan het bewustzijn van medewerkers met betrekking tot het belang van een goede logische toegangsbeveiliging. De volgende zaken zijn van belang:

- Gebruikersnamen en wachtwoorden zijn strikt persoonlijk. Onderlinge uitwisseling mag niet plaatsvinden.
- Wachtwoorden dienen geheim te blijven. Bijvoorbeeld een briefje met daarop het wachtwoord opgeschreven en aan de monitor geplakt, onder het toetsenbord of op een andere onveilige plaats bewaard, is niet toegestaan. Het door kwaadwillende proberen te achterhalen van gebruikersnamen en wachtwoorden door middel van phishing[10], shoulder surfing[11] en social engineering[12] aanvallen.

Objecten

De objecten binnen logische toegangsbeveiliging zijn:

- De informatie/gegevens die zijn vastgelegd met behulp van geautomatiseerde hulpmiddelen.
- De geautomatiseerde informatiesystemen.
- De omgevingen (ontwikkeling/test/acceptatie/productie) aanwezig op de computersystemen.
- De besturingssystemen en databasemanagementsysteem (DBMS) aanwezig op de computersystemen.
- De hulpmiddelen (ontwikkel- en querytools[13]) aanwezig op de computersystemen.
- De netwerken en infrastructuur (inclusief hardware) waarmee toegang tot computersystemen wordt verkregen.

[8] https://www.digid.nl/
[9] https://www.eherkenning.nl/
[10] Bij phishing wordt gebruik gemaakt van een e-mail waarbij de eindgebruiker wordt verleid om zijn gebruikersgegevens, waaronder het wachtwoord, in te vullen op een malafide website.
[11] Meekijken met het invoeren van wachtwoorden.
[12] Een social engineer zal proberen gebruikersgegevens te krijgen door zich bijvoorbeeld voor te doen als helpdeskmedewerker. Er wordt dus gewoon om wachtwoord en gebruikersgegevens gevraagd en vaak gekoppeld aan een probleem dat moet worden opgelost.
[13] Querytools worden gebruikt voor het beheren en uitvoeren van query's voor databasemanagementsystemen.

Maatregelen

Voor het beheersen van toegang tot gegevens dienen maatregelen genomen te worden. Deze maatregelen kunnen worden gecategoriseerd naar de aard van de maatregel. Hierbij worden beheersingsmaatregelen onderscheiden in organisatorische, procedurele en technische beheersingsmaatregelen.

De organisatorische beheersingsmaatregelen richten zich op het structureren van een organisatie. Bij logische toegangsbeveiliging kan men hierbij denken aan hoe de verantwoordelijkheid voor de gebruikersrechten binnen de gemeente is belegd. In beginsel mag niemand autorisaties hebben om een gehele cyclus van handelingen in een informatiesysteem te beheersen, zodanig dat beschikbaarheid, integriteit of vertrouwelijkheid kan worden gecompromitteerd. Indien dit toch noodzakelijk is, dient een audit trail[14] te worden vastgelegd van alle handelingen en tijdstippen in het proces, dusdanig dat de transactie kan worden herleid. De audit trail is niet toegankelijk voor degene wiens handelingen worden vastgelegd. Er is een scheiding tussen beheertaken en overige gebruikstaken. Beheerwerkzaamheden worden alleen uitgevoerd wanneer ingelogd als beheerder, normale gebruikstaken alleen wanneer ingelogd als gebruiker.

De procedurele maatregelen voor het toekennen, wijzigen, opschorten en intrekken van rechten van gebruikers spelen een belangrijke rol bij logische toegangsbeveiliging.

Bij de technische beheersingsmaatregelen gaat het om de daadwerkelijke gebruikersprofielen en de daarbij horende objecten, bijvoorbeeld bestanden en informatiesystemen. Voorbeelden van technische beheersingsmaatregelen zijn:

- Groepen informatiediensten, gebruikers en informatiesystemen worden op het netwerk gescheiden zodat de kans op onbevoegde toegang tot gegevens verder wordt verkleind.
- Het gebruik van informatiesystemen, alsmede uitzonderingen en informatiebeveiligingsincidenten, worden vastgelegd in logbestanden op een manier die in overeenstemming is met het risico, en zodanig dat tenminste wordt voldaan aan alle relevante wettelijke eisen. Relevante zaken om te loggen zijn:
    - Type gebeurtenis (zoals reset wachtwoord)
    - Handelingen met speciale bevoegdheden
    - (Poging tot) ongeautoriseerde toegang
- Een logregel (record) bevat minimaal:
    - Een tot een natuurlijk persoon herleidbare gebruikersnaam of gebruikers-ID[15]
    - De gebeurtenis
    - Waar mogelijk, de identiteit van het werkstation of de locatie
    - Het object waarop de handeling werd uitgevoerd
    - Het resultaat van de handeling
    - De datum en het tijdstip van de gebeurtenis

Voordelen logische toegangsbeveiliging

Op het moment dat logische toegangsbeveiliging goed is ingericht en wordt onderhouden levert dat de gemeente een aantal voordelen op. Dit zijn onder andere:

[14] Een audit trail (ook wel audit log) is een vanuit beveiligingsoogpunt relevant chronologisch verslag. Een audit trail bestaat uit een verzameling records (logregels) die als bewijsstuk dienen van de opeenvolging van activiteiten die invloed hebben gehad op een specifieke operatie, procedure of gebeurtenis.
[15] Een gebruikers-ID is een unieke identificatie van een account waarmee één gebruiker in uw gemeente wordt vertegenwoordigd.

- Inzichtelijkheid
  Gemeenten hebben op basis van wetgeving en gegevensleveringsovereenkomsten[16] toegang tot GBA en Suwinet. Deze wetgeving en gegevensleveringsovereenkomsten stellen eisen aan de maatregelen die gemeenten dienen te implementeren om aan te tonen dat de organisatie de belangrijkste risico's binnen haar bedrijfsprocessen beheerst. Logische toegangsbeveiliging is vaak een van de beheersmaatregelen waar een gemeente op steunt. Een gemeente moet dan ook in staat zijn om aan te tonen dat de toegangsrechten in een informatiesysteem tijdig en juist zijn geïmplementeerd. Zo dient er geen gebruik gemaakt te worden van ongepersonaliseerde accounts en dienen gebruikers over niet meer rechten te beschikken dan zij voor hun werkzaamheden nodig hebben. Het gebruik maken van gepersonaliseerde accounts en geen 'algemene' identiteiten zorgt ook voor onloochenbaarheid/onweerlegbaarheid[17].
- Transparantie
  Een tweede reden is dat logische toegangsbeveiliging en in het bijzonder de regel geen gebruik te maken van 'algemene' (ongepersonaliseerde) identiteiten, herleidbaarheid en transparantie mogelijk maakt. Hiervoor is het namelijk nodig om te weten wie een bepaalde actie heeft uitgevoerd. Transparantie is de mate van openheid, zichtbaarheid en toegankelijkheid van gemeenten naar haar burgers en (keten)partners. Dat leidt ertoe dat gemeenten achteraf in staat zijn verantwoording af te leggen over hun bedrijfsvoering.
- Effectiviteit
  De derde reden voor het beheersen van de logische toegangsbeveiliging heeft betrekking op de effectiviteit van het gebruikersbeheer in de gegevensverwerkende systemen. Een goed ingerichte logische toegangsbeveiliging stelt gemeenten in staat om medewerkers de juiste toegang te geven tot de benodigde gegevensverwerkende systemen of om de toegang van medewerkers te verwijderen. Goed ingericht gebruikersbeheer leidt er toe dat autorisaties accuraat worden afgehandeld, waardoor oneigenlijk gebruik zoveel mogelijk wordt tegen gegaan.
- Efficiëntie
  De laatste reden voor het beheersen van de logische toegangsbeveiliging kan gezocht worden in efficiëntie. Er kunnen kostenbesparingen plaatsvinden zowel in de primaire bedrijfsprocessen als in de ondersteunende diensten. Bij een goede logische toegangsbeveiliging kunnen medewerkers eerder aan de slag door een snellere afhandeling van wijzigingsverzoeken bij het gebruikersbeheer. De tweede besparing vindt plaats in de gebruikersbeheerprocessen. Door de gebruikersbeheerprocessen efficiënt in te richten zullen minder handelingen nodig zijn van de medewerkers waardoor de totale kosten van het gebruikersbeheer afnemen.

[16] Een gegevensleveringsovereenkomst wordt afgesloten tussen de systeemeigenaar van het bronsysteem en de afnemer van de gegevens.
[17] De eigenschap (van een bericht) om aan te tonen dat bepaalde gebeurtenissen of handelingen hebben plaatsgevonden, zoals het verzenden en ontvangen van elektronische documenten.

3 Beleid logische toegangsbeveiliging

3.1 Algemeen

Met de steeds toenemende automatisering en de toenemende nadruk op veiligheid en integriteit wordt de vraag 'wie is gemachtigd welke handelingen in een bepaald geautomatiseerd informatiesysteem te verrichten?' van steeds groter belang.
Gemeenten hebben op basis van wetgeving en gegevensleveringsovereenkomsten toegang tot GBA en Suwinet. Deze toegang is beperkt tot die taken waarvoor wettelijke grondslag en doelbinding van gegevensgebruik is vastgesteld. De toegangsrechten zijn ingericht in zogenaamde autorisatierollen. Gemeenten bepalen zelf welke medewerkers een autorisatierol krijgen voor GBA en Suwinet, uiteraard binnen de wettelijke kaders en met in achtneming van doelbinding en proportionaliteit. Gemeenten dienen dit ook in te richten voor de eigen informatiesystemen. Daarom is het voorliggende 'Beleid logische toegangsbeveiliging' opgesteld.
In bijlage 1 en 2 is respectievelijk een voorbeeld beleid logische toegangsbeveiliging en een voorbeeld autorisatieprocedure uitgewerkt. Het voorbeeld beleid logische toegangsbeveiliging en autorisatieprocedure hebben een hoog abstractieniveau. Het beleid logische toegangsbeveiliging geeft aan de eigenaar van een geautomatiseerd informatiesysteem de opdracht om voor zijn informatiesysteem een autorisatiesystematiek (autorisatieprocedure) in te regelen, conform de eisen en randvoorwaarden van het overkoepelende gemeentelijke voorbeeld informatiebeveiligingsbeleid.

Uitgangspunten
Uitsluitend bevoegde personen hebben toegang tot en kunnen gebruik maken van informatiesystemen en/of gegevens. De bevoegdheid van een persoon moet worden afgeleid van de taak, functie of verantwoordelijkheid van de betreffende persoon, dit ter beoordeling van de systeem- en/of gegevenseigenaar, op aangeven van een autorisatiebevoegde medewerker. Afhankelijk van de dataclassificatie dienen medewerkers een geheimhoudingsverklaring te ondertekenen.[18]

Definities
In deze regeling worden de volgende definities gehanteerd.

- **Beleid logische toegangsbeveiliging**: De uitgangspunten die de gemeente hanteert bij het regelen van een beheerste toegang tot, en gebruik van, een informatiesysteem.
- **Autoriseren in het kader van het beleid logische toegangsbeveiliging**: Iemand een bevoegdheid geven tot het wijzigen van het informatiesysteem zelf, of tot het wijzigen of raadplegen van de inhoud van het informatiesysteem.

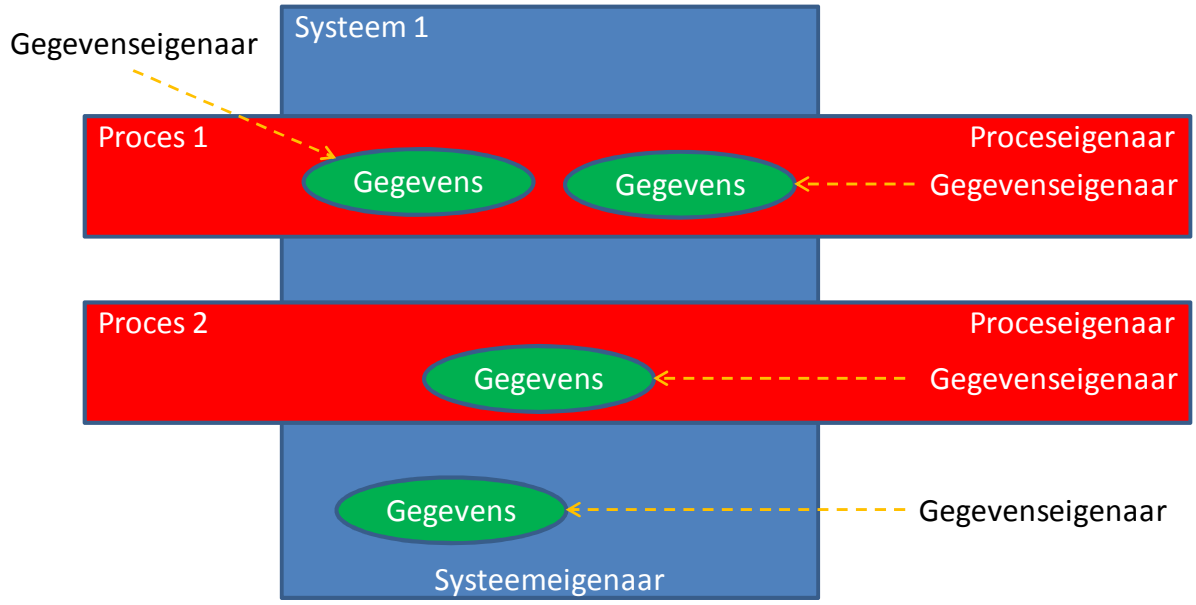
Naast bovengenoemde definities kent de gemeente ook nog het eigenaarschap van het informatiesysteem, van de gegevens in het informatiesysteem en van de processen rond het informatiesysteem.

- De **systeemeigenaar** is verantwoordelijk voor het juist functioneren van het informatiesysteem.
- De **gegevenseigenaar** is verantwoordelijk voor de juistheid van de gegevens in het informatiesysteem in kwestie.

[18] Zie hiervoor ook het operationele product 'Geheimhoudingsverklaringen' van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG).

- De **proceseigenaar** is verantwoordelijk voor het goed functioneren van de processen die een wisselwerking hebben met het informatiesysteem.

Uit bovenstaande definities volgt dat de systeemeigenaar, de gegevens- en proceseigenaar tot klant heeft. De gegevenseigenaar en de proceseigenaar bepalen hoe de gegevens en de processen eruit zien. Vervolgens dient de systeemeigenaar het informatiesysteem hierop in te richten. In figuur 1 wordt deze samenhang schematisch weergegeven.



Figuur 1. Samenhang systeem-, gegevens- en proceseigenaar

Verantwoordelijkheden

1. Met betrekking tot het beleid logische toegangsbeveiliging worden de volgende functionarissen onderkend:
   - College van burgemeester en wethouders (B&W)
   - Lijnmanagers
   - Systeem-, gegevens-, en proceseigenaren
   - Chief Information Security Officer (CISO)
   - Interne accountantsdienst (gemeentelijke auditors)
2. Het college van burgemeester en wethouders (B&W) keurt het beleid formeel goed en draagt zorg voor de naleving van het beleid in de gemeente (Beleidsbepaling).
3. De lijnmanagers zijn verantwoordelijk voor een correcte naleving van het beleid door hun medewerkers (Beleidsuitvoering).
4. De Chief Information Security Officer (CISO) is verantwoordelijk voor het voorbereiden en opstellen van het beleid logische toegangsbeveiliging (Beleidsvoorbereiding). De CISO coördineert de implementatie (Coördinatie) van het beleid.
5. Het eigenaarschap van systemen, gegevens en processen is belegd bij personen in de gemeente. De eigenaren zijn verantwoordelijk voor het treffen en in stand houden van de autorisatiemaatregelen (Beleidsinrichting). De gegevenseigenaren zijn verantwoordelijk voor de beveiliging van de onder hun ressorterende gegevens. De gegevens-, systeem- of proceseigenaren verlenen de toestemming aan gebruikers tot gebruik van de onder de verantwoordelijkheid van de eigenaar ressorterende gegevens, systemen en processen

(toewijzen van de autorisaties). Deze verleende rechten worden in een autorisatiematrix vastgelegd (zie bijlage 5: Voorbeeld autorisatieoverzichten).

6. De CISO is primair verantwoordelijk voor de controle op het beleid logische toegangsbeveiliging en een controle op een juiste uitvoering van het beleid door de gemeente (Beleidscontrole). Hieronder valt ook het controleren van de autorisatiematrix. De CISO kan hiertoe de in- of externe accountantsdienst opdracht geven. De interne accountantsdienst is gemachtigd om op eigen initiatief, steekproefsgewijs, controles uit te voeren op het beleid logische toegangsbeveiliging en een controle op een juiste uitvoering van het beleid door de gemeente (Beleidscontrole).

	College van B&W	**CISO**	**Systeem-, gegevens- en proceseigenaren**	**Lijnmanagers**	**Interne accountantsdienst (gemeentelijke auditors)**
Beleidsvoorbereiding		**X**			
Beleidsbepaling	**X**				
Coördinatie		**X**			
Beleidsinrichting			**X**		
Beleidsuitvoering				**X**	
Beleidscontrole		**X**			**(X)**

Tabel 1. Verantwoordelijkheden met betrekking tot het beleid logische toegangsbeveiliging

Randvoorwaarden

Onderstaande randvoorwaarden dienen ingevuld te worden met betrekking tot de logische toegangsbeveiliging procedures:

- Er is een overzicht van informatiesystemen beschikbaar.
  Dit overzicht bevat de informatiesystemen die bij de gemeente beschikbaar zijn (zie bijlage 4: Voorbeeld overzicht van informatiesystemen) en voor ieder informatiesysteem wordt aangegeven wie de systeemeigenaar is. Op het moment dat de gemeente beschikt over een configuratiebeheersysteem (CMDB)[19], dan zijn deze gegevens in deze CMDB vastgelegd en hoeft geen afzonderlijk overzicht te worden bijgehouden.[20]
- Er is een overzicht van autorisatiebevoegde medewerkers beschikbaar.
  Dit overzicht bevat de personen die geautoriseerd (gemachtigd) zijn voor het aanvragen van toegang tot het informatiesysteem en/of gegevens. Dit overzicht wordt opgesteld en actueel gehouden door de systeemeigenaar, eventueel in overleg met de gegevens- en/of proceseigenaar. Het kan ook zijn dat de direct leidinggevende van de medewerker geautoriseerd is voor het aanvragen van toegang tot het informatiesysteem en/of gegevens.
- Er is een overzicht van wel en niet toegestane combinaties van taken beschikbaar.
  Deze matrix bevat een overzicht van wel en niet toegestane combinaties van autorisaties binnen een informatiesysteem, die aan één medewerker mogen worden toegekend (zie bijlage 5: Voorbeeld autorisatieoverzichten). In deze lijst dienen de rollen voor te komen die uit het oogpunt van functiescheiding belangrijk zijn. Dit overzicht wordt opgesteld en actueel

[19] Een gegevensbestand dat wordt gebruikt om de configuratieregistraties op te slaan tijdens hun levenscyclus. Het configuratiebeheersysteem slaat attributen van configuratie-items op. Evenals relaties met andere configuratie-items. De Engelse benaming is configuration management database (CMDB).
[20] Zie ook de 'Handreiking proces configuratiebeheer' van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG).

gehouden door de systeemeigenaar, eventueel in overleg met de gegevens- en/of proceseigenaar.

- Er is een overzicht, met daarin welke functies worden uitgevoerd door welke medewerker, beschikbaar.
  Deze autorisatiematrix bevat een overzicht van welke autorisaties aan één medewerker zijn toegekend (zie bijlage 5: Voorbeeld autorisatieoverzichten). Dit dient minimaal per informatiesysteem of bedrijfsproces te worden geadministreerd, maar kan afhankelijk van de grootte en complexiteit van de gemeente ook afdelingsbreed worden vastgelegd. Dit overzicht wordt opgesteld en actueel gehouden door de systeem-, proceseigenaar of afdelingsmanager.
- Er is een overzicht van autorisatiebeheerders beschikbaar.
  Dit overzicht bevat de personen die geautoriseerd (gemachtigd) zijn voor het aanmaken van gebruikers en het verlenen van toegang tot informatiesystemen en/of gegevens. Bijvoorbeeld de volgende verdeling van verantwoordelijkheden voor het aanvragen en toekennen van autorisaties binnen informatiesystemen:
  - Lijnmanagement: Aanvragen autorisaties voor nieuwe gebruikers (zie hiervoor het overzicht van autorisatiebevoegde medewerkers).
  - Functioneel beheerder / Servicedesk: Toewijzen en controleren van autorisatieaanvragen.
  - Applicatiebeheerder: Technische realisatie van de aanvragen binnen de informatiesystemen (in de gebruikersadministratie).
  - Technisch beheerder: Technische realisatie van de aanvragen binnen de computersystemen (in de gebruikersadministratie).
- Het toekennen van speciale bevoegdheden aan medewerkers, veelal technische beheerders en ontwikkelaars, die bevoegd zijn speciale tools te gebruiken vindt beperkt plaats. Gebruik van deze speciale bevoegdheden wordt door logging afzonderlijk vastgelegd.
- Medewerkers worden geïdentificeerd door middel van een gebruikersnaam. De gebruikersnaam dient te voldoen aan de geldende naamgevingsconventie die van toepassing zijn in de gemeente. Als medewerkers worden geauthenticeerd door middel van een wachtwoord, dan dient het wachtwoord te voldoen aan de door de gemeente vastgestelde eisen.[21]

Beheer

Logische toegangsbeveiliging kan niet effectief worden ingevoerd als het beheer aspect niet wordt ingevuld. Vandaar dat hier een beschrijving wordt gegeven van de verschillende organisatorische maatregelen waaraan aandacht dient te worden besteed om een techniek voor toegangsbeveiliging effectief te maken. Dit wordt beschreven aan de hand van procedures, die een gemeente in het kader van logische toegangsbeveiliging minimaal dient te beschrijven. Er dienen procedures beschreven te worden voor het aanvragen, wijzigen, opschorten en intrekken van rechten (autorisaties).

Er is een procedure aanwezig, bedoeld ter ondersteuning van beheerders, die aangeeft op welke wijze en in welke situatie gebruikers geautoriseerd worden om gebruik te maken van het informatiesysteem. De procedure 'Aanvragen of wijzigen autorisaties' bevat op hoofdlijnen de volgende stappen (zie figuur 2, pagina18):

1. Een autorisatiebevoegde medewerker dient met behulp van het daarvoor bestemde aanvraag- of wijzigingsformulier schriftelijk een autorisatieverzoek in voor een nieuwe of gewijzigde autorisatie bij de servicedesk[22].

[21] Zie ook het 'Wachtwoordbeleid' van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG).
[22] De servicedesk is een centrale afdeling in een ICT- of facilitaire organisatie. Een vergelijkbare afdeling in een organisatie is het callcenter of helpdesk. Het grote verschil tussen een servicedesk en een helpdesk, is dat ze Bij de helpdesk een probleem meestal alleen registreren en oplossen of doorsturen naar een tweede lijn. Bij

2. De servicedesk beoordeelt het autorisatieverzoek. De servicedesk dient de aanvragen te beoordelen waarbij in ieder geval wordt gecontroleerd of:
   - Het aanvraag- of wijzigingsformulier volledig en op de juiste manier is ingevuld (zie bijlage 6: Voorbeeld autorisatie aanvraagformulier).
   - Het aanvraag- of wijzigingsformulier door een autorisatiebevoegde medewerker is ingediend (ondertekend). Op het moment dat aanvragen ook per e-mail (digitaal) mogen worden ingediend, dient uiteraard gecontroleerd te worden of de afzender bevoegd is om deze aanvraag in te dienen. Tevens dient gecontroleerd te worden of de e-mail ook daadwerkelijk door de afzender is verstuurd (eventueel steekproefsgewijs).
   - Het autorisatieverzoek in overeenstemming is met de beveiligingseisen zoals vastgelegd in het overzicht van wel en niet toegestane combinaties van taken, zodat er geen met elkaar conflicterende bevoegdheden ontstaan, die niet aan één gebruiker gekoppeld mogen worden (geen functiescheiding) (zie bijlage 5: Voorbeeld autorisatieoverzichten).

   Bovenstaande toetsingspunten dienen zichtbaar te zijn uitgevoerd. Er dient vastgelegd te worden wie toegang heeft tot welk informatiesysteem en/of gegevens, hierbij dient tevens aangegeven te worden welke bevoegdheden een medewerker heeft. De servicedesk registreert deze aanvraag of wijziging in een registratiesysteem en voegt daar de originele aanvraag bij.
3. De autorisatiebeheerder die het autorisatieverzoek van de servicedesk ontvangt regelt de autorisaties en geeft een melding terug aan de servicedesk als het autorisatieverzoek is afgehandeld.
4. De servicedesk koppelt aan de autorisatiebevoegde medewerker en de betrokken medewerker (gebruiker) terug dat het autorisatieverzoek is afgehandeld. De servicedesk sluit de bijbehorende registratie af.

Aanvraag autorisatie
Er is een procedure aanwezig die aangeeft op welke wijze en in welke situatie gebruikers geautoriseerd worden om gebruik te maken van het object van logische toegangsbeveiliging.

Er is een overzicht (autorisatiematrix) aanwezig waaruit per functie blijkt welke autorisaties bij de betreffende functie behoren. Bij het opstellen daarvan is rekening gehouden met de noodzakelijke functiescheiding en het need-to-know[23] principe. Dit overzicht is vastgesteld door de leiding. Het verstrekken van autorisaties vindt plaats op basis van de situatie dat medewerkers in dienst treden, een functiewijziging plaatsvindt dan wel medewerkers uit dienst treden. Autorisaties worden verstrekt op basis van zakelijke behoeften met als uitgangspunt 'niet nodig, tenzij'. Indien door een te geringe personele capaciteit functiescheiding onmogelijk is, kan hier, onder bepaalde omstandigheden tijdelijk vanaf worden afgeweken. Zie hiervoor bijlage 3: Voorbeeld procedure ontbreken voldoende functiescheiding.

De procedure 'Aanvraag tot autorisaties' dient uitgewerkt te worden in de volgende subprocedures: aanvragen, vrijgeven, blokkeren en verwijderen.

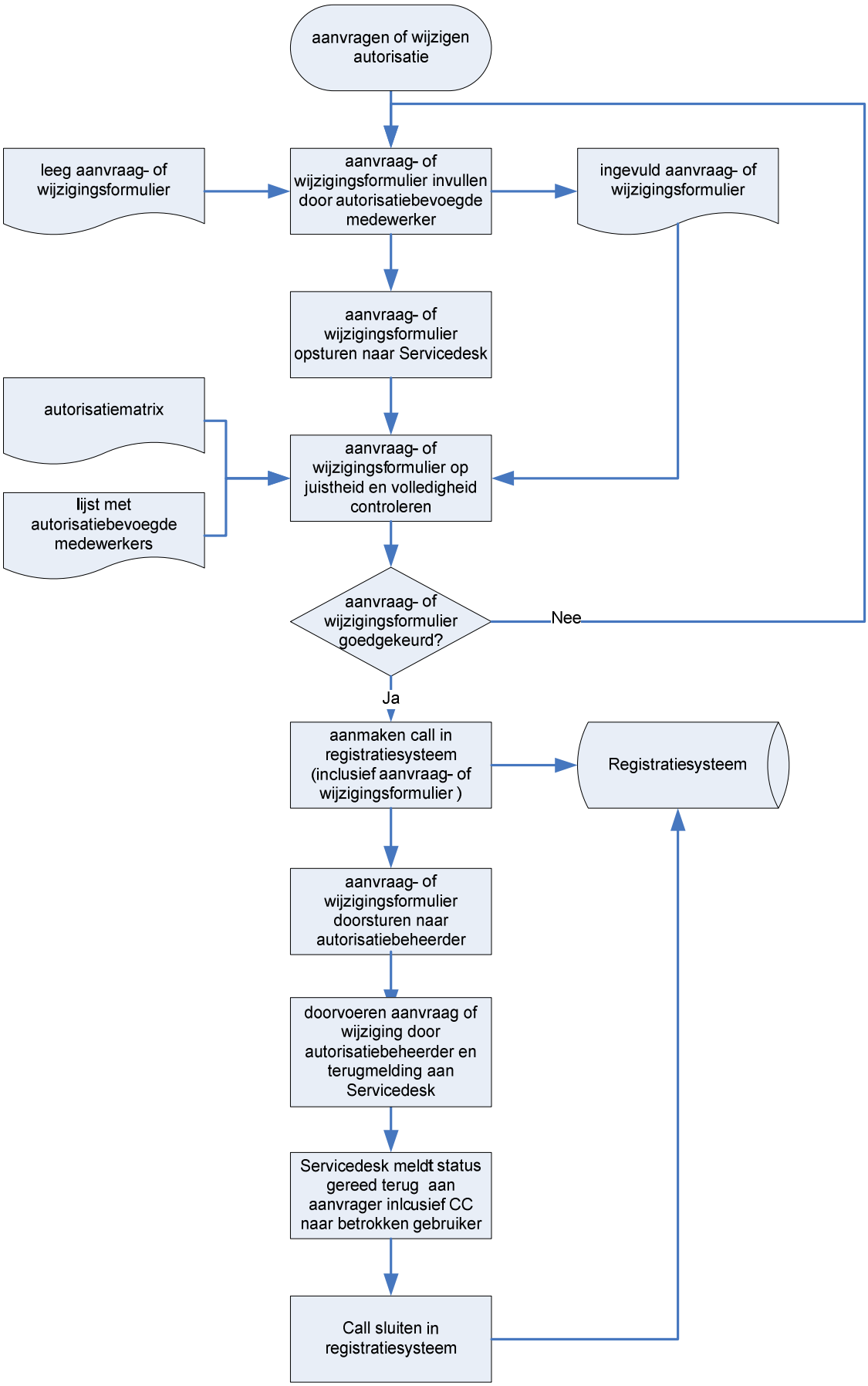
Autorisatieaanvragen dienen bij binnenkomst te worden geregistreerd en de volgende gegevens te bevatten: naam aanvrager, gebruiker/begunstigde, aanvraagdatum, gewenste ingangsdatum, einddatum (bij tijdelijke medewerkers), gewenste bevoegdheden.

<u>Procedure uitgifte gebruiker-ID's</u>

een servicedesk ligt de dienstverlening hoger. Op een servicedesk worden bijvoorbeeld ook autorisaties verleend en ICT-gerelateerde bestellingen aangenomen. (Bron: http://nl.wikipedia.org/wiki/Servicedesk)
[23] Toegang tot de informatie moet noodzakelijk zijn voor het uitvoeren van officiële taken.

Om het identificatieproces mogelijk te maken, dienen gebruikers bekend te zijn in het informatiesysteem. In een procedure die dit regelt, dient het volgende beschreven te zijn:

- Hoe een medewerker kenbaar maakt dat hij gebruik wil maken van een bepaald informatiesysteem. Bijvoorbeeld via een aanvraagformulier of een informatiesysteem voor het doen van een digitale aanvraag.
- Welke gegevens bij een aanvraag ingevuld dienen te worden. Bijvoorbeeld persoonsgegevens van de betrokken medewerker en informatie waaruit blijkt dat de gebruiker uit hoofde van zijn functie inderdaad een gebruikers-ID nodig heeft.
- Door wie en hoe een gebruikers-ID in het informatiesysteem wordt ingevoerd. Bijvoorbeeld de functioneel beheerder, applicatiebeheerder of systeemeigenaar.
- Waar, hoe en hoelang deze aanvragen worden bewaard. Bijvoorbeeld tot 3 maanden na intrekking van de bevoegdheden of een wettelijke bewaartermijn.



Figuur 2. Procedure aanvragen of wijzigen autorisatie.

Procedure uitgifte van rechten (autorisaties)

Om het autorisatieproces mogelijk te maken, dienen de rechten van een gebruiker bekend te zijn in het informatiesysteem. Vaak wordt deze procedure gecombineerd met de procedure uitgifte gebruikers-ID. In een procedure die dit regelt, dient het volgende beschreven te zijn:

- Hoe de aanvrager (bijvoorbeeld de manager) kenbaar maakt welke rechten de medewerker/gebruiker dient te hebben in een bepaald informatiesysteem. Bijvoorbeeld via een aanvraagformulier of een informatiesysteem voor het doen van een digitale aanvraag.
- Welke gegevens bij de aanvraag ingevuld dienen te zijn. Bijvoorbeeld informatie waaruit blijkt dat de gebruiker uit hoofde van zijn functie inderdaad de rechten nodig heeft.
- Door wie en hoe rechten in het informatiesysteem worden ingevoerd. Bijvoorbeeld de functioneel beheerder, applicatiebeheerder of systeemeigenaar.
- Waar, hoe en hoelang deze aanvragen worden bewaard. Bijvoorbeeld tot 3 maanden na intrekking van de bevoegdheden, een wettelijke bewaartermijn of de bewaartermijn van de auditlogging, zodat je kunt zien wie bevoegd was.

Procedure mutatie van rechten (autorisaties)

Aangezien gebruikers binnen een organisatie van functie kunnen veranderen, dienen rechten van gebruikers in het informatiesysteem te worden gewijzigd casu quo te worden verwijderd. In een procedure die dit regelt, dient het volgende beschreven te zijn:

- Wanneer rechten van een gebruiker worden gewijzigd. Bijvoorbeeld in verband met een andere functie.
- Door wie en hoe mutaties worden uitgevoerd. Bijvoorbeeld de functioneel beheerder, applicatiebeheerder of systeemeigenaar.
- Waar, hoe en hoelang de mutaties in de administratie worden vastgelegd. Bijvoorbeeld tot 3 maanden na intrekking van de bevoegdheden, een wettelijke bewaartermijn of de bewaartermijn van de auditlogging, zodat je kunt zien wie bevoegd was.

Procedure opschorten of intrekken van gebruiker-ID’s

Aangezien gebruikers de organisatie verlaten of van functie veranderen, dienen gebruikers uit het informatiesysteem te worden verwijderd. In een procedure die dit regelt, dient het volgende beschreven te zijn:

- Wanneer en hoe een gebruiker wordt afgemeld. Bijvoorbeeld in verband met een andere functie, pensioen, andere werkgever of ontslag.
- Wie verantwoordelijk is voor het intrekken van gebruikers-ID’s. Bijvoorbeeld de direct leidinggevende van de medewerker of de afdeling Personeel & Organisatie (P&O). Hierbij kan onderscheid zijn in interne en externe (inhuur) medewerkers van de gemeente.
- Wie verantwoordelijk is voor het opschorten van gebruikers-ID’s. Bijvoorbeeld de direct leidinggevende van de medewerker indien gedurende een langere periode geen gebruik van een gebruikers-ID wordt gemaakt.
- Door wie en hoe een gebruikers-ID uit het informatiesysteem wordt verwijderd.
- Waar, hoe en hoelang dit in de administratie dient te worden vastgelegd. Bijvoorbeeld tot 3 maanden na intrekking van de bevoegdheden, een wettelijke bewaartermijn of de bewaartermijn van de auditlogging, zodat je kunt zien wie bevoegd was.

Procedure intrekken van rechten (autorisaties)

Verondersteld wordt dat de rechten van een bepaalde gebruiker uit het informatiesysteem verdwijnen als het gebruikers-ID van een bepaalde gebruiker wordt ingetrokken, zodat hiervoor geen aparte procedure hoeft te worden opgesteld (zie de procedure opschorten of intrekken van gebruikers-ID’s).

Toegang gebruikersdatabase
Daar niet iedereen toegang zal hebben tot de gebruikersdatabase is het raadzaam een procedure op te stellen die de toegang tot de database regelt. In een procedure die dit regelt, dient het volgende beschreven te zijn:

- Welke functionaris (in dit document wordt uitgegaan van een autorisatiebeheerder) toegang heeft tot de database.
- Welke werkzaamheden door deze functionaris worden uitgevoerd.

Vervanging van de autorisatiebeheerder
Deze procedure regelt de vervanging van de autorisatiebeheerder, indien deze zijn wachtwoord vergeten is of afwezig is. In een procedure die dit regelt, dient het volgende beschreven te zijn:

- Wat de vervangingsprocedure in houdt
- Waar deze vervangingsprocedure kan worden gevonden
- Wanneer en door wie deze mag worden aangesproken
- Welke werkzaamheden de vervanger mag uitvoeren

3.2 Controleren

Er is een procedure aanwezig voor periodieke[24] controle van het proces 'Logische toegangsbeveiliging' en hierover wordt aan het management gerapporteerd. Bij deze controle wordt de werkwijze ten aanzien van aanvragen, wijzigen en verwijderen van autorisaties nagegaan. Bij voorkeur worden deze controles uitgevoerd op alle informatiesystemen, maar minimaal op de informatiesystemen met de hoogste risico's, of waar dit wettelijk verplicht is.

De actuele stand van zaken van de toegekende autorisaties wordt periodiek gecontroleerd. Deze controle vindt plaats op geldigheid en rechtmatigheid van de verstrekte actuele autorisaties (medewerkers, gebruikersnamen, bevoegdheden). Over de resultaten van iedere periodieke controle wordt zowel aan de CISO als aan de relevante systeem-, gegevens-, en proceseigenaren gerapporteerd. Deze rapportage dient van de volgende onderdelen te zijn voorzien:

- Wie heeft de controle uitgevoerd?
    - De volledige naam, functie en voorzien van een (herleidbare) handtekening/paraaf
- Resultaten van de controle, die kan bestaan uit:
    - Autorisatie overzichten (voorzien van een productiedatum)
    - Een controledatum
    - De conclusie van de controle
- Aanbevelingen

Tijdens deze controle dient te worden vastgesteld dat de vastgestelde actuele autorisatiematrix in overeenstemming is met het, door de autorisatiebeheerder verstrekte, overzicht van autorisaties. Deze controle dient uitgevoerd te worden door een andere functionaris dan die verantwoordelijk is voor het operationaliseren van de logische toegangsbeveiliging/autorisatie. Indien dit toch noodzakelijk is dan wordt door de systeemeigenaar apart toezicht georganiseerd op de betreffende functionaris.

Jaarlijks vindt in opdracht van de CISO een interne controle plaats. De CISO kan deze uit laten voeren door de interne accountantsdienst. Deze interne controle wordt niet door beheerders

[24] Bijvoorbeeld per kwartaal, maar dit is afhankelijk van de grootte van de gemeente en het object van logische toegangsbeveiliging.

uitgevoerd om zoveel mogelijk beïnvloeding van het resultaat te beperken. De volgende onderwerpen maken onderdeel uit van de interne controle:

Opzet: Zijn de procedures aanwezig?

- Vaststellen dat de logische toegangsbeveiligingsprocedures aanwezig en actueel zijn.
- Vaststellen dat de volgende overzichten per informatiesysteem aanwezig en actueel zijn (mits van toepassing)[25]:
    - Overzicht van autorisatiebevoegde medewerkers
    - Overzicht van wel en niet toegestane combinaties van taken
    - Overzicht welke taken behoren bij een specifieke functie
    - Overzicht welke functies worden uitgevoerd door een medewerker

Bestaan en Werking: Zijn de processen aanwezig en werken ze zoals bedoeld?

- Vaststellen dat de logische toegangsbeveiligingsprocedures, op alle betreffende elementen, correct en volledig zijn toegepast.
- Vaststellen dat de doorgevoerde wijzigingen zijn geautoriseerd, aanwezigheid van functiescheiding, autorisatie (functies) corresponderen met de functionaris.
- Vaststellen dat uitsluitend de bevoegde personen autorisatie hebben gekregen.
- Vaststellen dat per mutatie het proces van aanvraag tot uiteindelijke toekenning/wijziging van autorisaties kan worden getraceerd.
- Vaststellen dat de procedures met betrekking tot autorisaties zijn nageleefd en vaststellen dat deze inhoudelijk juist zijn uitgevoerd (in overeenstemming met de werkelijkheid) en dat alle mutaties via de geldende procedures zijn afgehandeld.
- Vaststellen dat de in het informatiesysteem geïmplementeerde autorisaties nog actueel gelden. Alle bevoegdheidsprofielen zijn nagekeken aan de hand van de meest actuele personeelslijst.
- Vaststellen dat in het geval van te verwijderen autorisaties en tijdelijke autorisaties (zogenaamde autorisaties met einddatum bestemd voor tijdelijke medewerkers) dit heeft plaatsgevonden op de aangegeven data.
    - Dit om vast te kunnen stellen dat er geen ongeautoriseerde handelingen hebben plaatsgevonden.
- Vaststellen dat de in het informatiesysteem geïmplementeerde autorisaties direct zijn aangepast bij wijziging van taken en of bij ontslag casu quo vertrek van (tijdelijke) medewerkers direct de autorisaties zijn geblokkeerd.[26]
- Vaststellen dat in het geval van het verwijderen van autorisaties, de opdrachten tot verwijderen voor de datum van implementatie ligt.
- Vaststellen dat in het geval van toekennen van een tijdelijke autorisatie, de opdracht daartoe voor de daadwerkelijke implementatiedatum ligt.
- Vaststellen dat de daadwerkelijk in het informatiesysteem geïmplementeerde autorisaties overeenkomen met de autorisaties zoals schriftelijk toegekend en vermeld op het individuele autorisatie aanvraagformulier.
- Vaststellen of ongeautoriseerde wijzigingen van autorisaties hebben plaatsgevonden. Hiervoor dient periodiek een autorisatieoverzicht van alle gebruikers te worden geproduceerd en door de verantwoordelijke functionaris te worden gecontroleerd.
    - Dit autorisatieoverzicht dient per gebruiker aan te geven waartoe deze is geautoriseerd.

[25] Zie onderdeel randvoorwaarden in paragraaf 3.1 algemeen door wie deze overzichten dienen te zijn opgesteld en actueel te worden gehouden.
[26] Afhankelijk van het informatiesysteem moet de medewerker hierbij zijn uitgelogd, wil dit effect hebben.

- Tijdens deze controle dient te worden gecontroleerd of er ongeautoriseerde wijzigingen zijn doorgevoerd (ongeautoriseerde wijzigingen zijn wijzigingen waarvoor geen volledig ingevuld aanvraagformulier aanwezig is of door een niet geautoriseerde medewerker is ingediend).
- Tijdens deze controle dient te worden gecontroleerd of de vastgestelde actuele autorisatiematrix in overeenstemming is met het autorisatieoverzicht.

Uitvoeren controles

- Vaststellen dat periodieke controles zijn uitgevoerd aan de hand van een rapportage en dossiervorming.
- Vaststellen of een medewerker (gebruiker) meerdere gebruikersnamen heeft. Indien dit het geval is, vaststellen dat dit met instemming van de leiding is en wat de reden is voor twee of meerdere gebruikersnamen.
- Vaststellen of alle geautoriseerden nog in dienst zijn en/of nog dezelfde functie vervullen als waarvoor men is geautoriseerd.
- Vaststellen of de functiescheiding is doorbroken. Indien dit het geval is, vaststellen dat de functiescheiding bewust, met instemming van de leiding, is doorbroken en of dit schadelijke gevolgen kan hebben.
- Vaststellen dat gebruikers die meerdere keren toegang tot het informatiesysteem proberen te krijgen, zonder gebruik te maken van de juiste gebruikersnaam en wachtwoord, door het informatiesysteem (al dan niet tijdelijk) zijn geblokkeerd.
- Vaststellen dat periodieke controle van en rapportage over medewerkers met speciale bevoegdheden, die tevens bevoegd zijn speciale tools te gebruiken, plaatsvindt.
- Vaststellen dat periodieke controle van en rapportage over ongeautoriseerde aanlogpogingen plaatsvindt.

3.3 Checklist logische toegangsbeveiliging

De checklist helpt gemeenten om te bepalen of het inrichten en onderhouden van de bescherming van informatiesystemen en de gegevens tegen ongeautoriseerde (logische) toegang en gebruik, voldoende beveiligd is op basis van maatregelen die als ‘good practice’ beschouwd worden.

1. De gemeente autoriseert en registreert gebruikers/beheerders die toegang hebben tot informatiesystemen op basis van een formele procedure waarin is opgenomen:
   - Het verlenen van toegang tot de benodigde gegevens op basis van de uit te voeren functie/taken.
   - Het uniek identificeren van elke gebruiker/beheerder tot één persoon.
   - Activiteiten zijn altijd te herleiden tot één persoon.
   - Het goedkeuren van de aanvraag voor toegangsrechten door de manager of een gemandateerde.
   - Het tijdig wijzigen (dus ook intrekken) van de autorisatie bij functiewijziging of vertrek.
   - Het benaderen van de databestanden door gebruikers mag alleen plaatsvinden via applicatieprogrammatuur (tenzij sprake is van calamiteiten).
2. Elke gebruiker/beheerder dient zich te authenticeren voordat er op een informatiesysteem activiteiten kunnen worden uitgevoerd.
3. Gebruikers- en beheeraccounts worden na een vast gedefinieerd aantal, bijvoorbeeld drie, foutieve/ongeldige inlogpogingen (al dan niet tijdelijk) geblokkeerd.

4. Er is een autorisatiematrix aanwezig, waarin gebruikers/beheerders, gebruik- en beheerprofielen en te beheren objecten beschreven worden en aan elkaar worden gekoppeld.
5. Gebruikers- en beheeraccounts zijn niet voorzien van meer rechten dan strikt noodzakelijk is voor het uitvoeren van de noodzakelijke taken.
6. Identificatie, authenticatie en autorisatie vinden plaats met behulp van een toegangbeveiligingstool. Bijvoorbeeld Identity & Access Management (I&AM).
7. Ongeautoriseerde toegangspogingen en essentiële activiteiten worden gedetecteerd, geanalyseerd en tegen inbreuken wordt actie ondernomen.
8. Controle op verleende toegangsrechten en gebruik van informatiesystemen en gegevens vindt meerdere keren per jaar plaats, in opdracht van de CISO of de systeem-, gegevens-, of proceseigenaren.
9. Het toepassen van schermbeveiligingsprogrammatuur (een screensaver) maakt na een periode van inactiviteit van maximaal 15 minuten alle informatie op het beeldscherm onleesbaar en ontoegankelijk.
10. Het gebruik van wachtwoorden is gebaseerd op het wachtwoordbeleid van de gemeente. Het binnen de gemeente geldende wachtwoordbeleid wordt, waar mogelijk, technisch afgedwongen.
11. Nadat een vooraf vastgestelde periode van inactiviteit is overschreden wordt de sessie automatisch afgesloten.
12. Beheersessies worden versleuteld.[27]
13. Beheerdiensten zijn netwerktechnisch enkel toegankelijk voor geautoriseerde beheerders.
14. Voordat er succesvol is ingelogd op een informatiesysteem, wordt een inlogbericht getoond, waarin wordt gewezen op het feit dat alle activiteiten op het informatiesysteem worden vastgelegd en waar nodig voor onderzoek en bewijsvoering kunnen worden overgedragen aan geselecteerde instanties.

[27] Een extra maatregel zou kunnen zijn om het beheer uit te voeren via een alternatieve, betrouwbare verbinding die een out-of-band verbinding wordt genoemd. Via deze verbinding hebben alleen de beheerders toegang.

Bijlage 1: Voorbeeld beleid logische toegangsbeveiliging gemeente <naam gemeente>

Het beleid logische toegangsbeveiliging is onderdeel van de informatiebeveiliging. Het beleid logische toegangsbeveiliging dient in lijn te zijn met de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) en zal moeten voldoen aan de wettelijke regelgevingen en beleidsdocumenten van <gemeente>.

1. De regeling beleid logische toegangsbeveiliging gemeente is van toepassing op informatiesystemen waarvan de gemeente eigenaar is. Ook als informatiesystemen niet binnen de gemeente draaien is deze regeling beleid logische toegangsbeveiliging van toepassing.[28]
2. De gemeente maakt, waar mogelijk, gebruik van bestaande (landelijke) voorzieningen voor authenticatie en autorisatie (voor burgers en bedrijfsleven gelden: DigiD en eHerkenning).
3. Voor elk bedrijfsproces, informatiesysteem, gegevensverzameling is een verantwoordelijke lijnmanager benoemd.
4. Iedere systeemeigenaar is verplicht tot het uitvoeren van een baselinetoets BIG en, afhankelijk van de uitkomsten van deze baselinetoets BIG, ook nog voor een diepgaande risicoanalyse voor de informatiesystemen waarvan hij eigenaar is.
5. Iedere systeemeigenaar is verplicht tot het maken van een specifieke autorisatieprocedure voor elk informatiesysteem waarvan hij eigenaar is.
6. Iedere systeemeigenaar is verplicht tot het toepassen van de specifieke autorisatieprocedures voor de informatiesystemen waarvan hij eigenaar is.
7. De systeemeigenaar dient bij het opstellen en uitvoeren van een specifieke autorisatieprocedure de volgende uitgangspunten te hanteren:
   - De autorisatiestructuur van een informatiesysteem is uniform voor de gehele gemeente.
   - De autorisatiestructuur van een informatiesysteem sluit aan bij de goedgekeurde procesbeschrijvingen.
   - Er worden in de regel geen ‘algemene’ (ongepersonaliseerde) identiteiten gebruikt.[29]
   - Gegevens worden alleen gemuteerd door de gegevenseigenaar of de daartoe, door de gegevenseigenaar, gemachtigde functionarissen.
   - De systeemeigenaar overlegt met de betrokken gegevenseigenaren en proceseigenaren over de vraag wie geautoriseerd wordt en op welke manier dat gebeurt.
   - De systeemeigenaar is verplicht de autorisatieprocedure te laten toetsen door de beveiligingsfunctionaris van de gemeente. Bijvoorbeeld de CISO.
8. De systeemeigenaar dient bij het opstellen van een autorisatieprocedure rekening te houden met mogelijk van toepassing zijnde wet- en regelgeving.
9. De systeemeigenaar moet bij het maken van een systeemspecifieke autorisatieprocedure aangeven welke detailnormen hij wel of niet van toepassing wil laten zijn. Bij detailnormen dient in het bijzonder gedacht te worden aan de volgende normen:
   - De gemeentelijke leidraad bij het opschonen van gegevens.
   - De gemeentelijk checklist voor het borgen van de betrouwbaarheid van gegevens.

[28] Denk aan een SaaS-oplossing, et cetera.
[29] Voor herleidbaarheid en transparantie is het namelijk nodig om te weten wie een bepaalde actie heeft uitgevoerd. Indien dit geen (wettelijke) eis is kan worden gewerkt met functionele accounts.

KWALITEITSINSTITUUT NEDERLANDSE GEMEENTEN IN OPDRACHT VAN VERENIGING VAN NEDERLANDSE GEMEENTEN

Functiescheiding

10. De beschikkende, bewarende en controlerende taken worden in beginsel nooit in één functionaris tezamen gebracht. Indien dit toch noodzakelijk is dan wordt door de systeemeigenaar apart toezicht georganiseerd op de betreffende functionaris.
11. (Technische) beheerders mogen geen toegang hebben tot de data van het informatiesysteem waar zij (technisch) beheerder van zijn. Indien dit toch noodzakelijk is dan wordt door de systeemeigenaar apart toezicht georganiseerd op de betreffende functionaris.[30]

Inhuur externen

12. De door de gemeente ingehuurde externen vallen onverkort onder het beleid logische toegangsbeveiliging en dienen conform deze regels te handelen.
13. Aan de hand van hun taken/functie zal hun toegang verleend worden tot de gegevens en informatiesystemen.

Uitbesteding aan een ICT-dienstverlener

14. De ICT-dienstverlener zal een beveiligingsbeleid moeten hebben en geëffectueerde maatregelen, die zij aan de gemeente inzichtelijk maakt.
15. De ICT-dienstverlener is verantwoordelijk voor een correcte inrichting van het beleid en naleving hiervan binnen de eigen organisatie. De ICT-dienstverlener voldoet aan de normen en eisen die gesteld zijn in het informatiebeveiligingsbeleid casu quo beleid logische toegangsbeveiliging en de van toepassing zijnde wet- en regelgeving.
16. Binnen de ICT-dienstverlener is een Securitymanager[31] aanwezig die verantwoordelijk is voor het informatiebeveiligingsbeleid van de ICT-dienstverlener en die contactpersoon is voor de CISO.
17. De normen en eisen aangaande de beveiliging maken onderdeel uit van het servicecontract (mantelovereenkomst, nadere overeenkomsten en diensten niveau overeenkomsten), dat tussen de gemeente en de ICT-dienstverlener afgesproken is.
18. De ICT-dienstverlener stelt uitsluitend in opdracht van de gemeente gegevens en systemen beschikbaar aan medewerkers uit de gemeente, de ICT-dienstverlener en aan derde partijen.
19. De ICT-dienstverlener stelt capaciteit en informatie beschikbaar aan audits op gebied van autorisaties, die in opdracht van de gemeente uitgevoerd worden.
20. Voor de dagelijkse operatie is er bij de ICT-dienstverlener een autorisatiebeheerder aanwezig die verantwoordelijk is voor een correcte inrichting van de autorisaties en die aanspreekpunt is voor de CISO. De autorisatiebeheerder ressorteert onder de Securitymanager.
21. De operationele afspraken en geldende procedures tussen opdrachtgever en ICT-dienstverlener worden vastgelegd in een dossier afspraken en procedures (DAP).

Beoordeling van de uitvoering van het beleid

22. De systeemeigenaar dient het toezicht op de uitvoering van de autorisatieprocedure goed te regelen en te documenteren. Hij neemt interne beheersmaatregelen die in overeenstemming zijn met de eisen die uit de baselinetoets BIG of risicoanalyse voortvloeien.
23. De uitvoering van het beleid logische toegangsbeveiliging wordt periodiek beoordeeld door de (interne) accountantsdienst. Het initiatief voor de uitvoering van de controles ligt bij de CISO of de systeem-, gegevens-, of proceseigenaren.

[30] Dit geldt ook voor functioneel beheer op het moment dat dit door een gemeente is uitbesteed aan een externe partij. Op het moment dat het hier over persoonsgegevens gaat dient de uitbestedingspartner een bewerkingsovereenkomsten te ondertekenen. Het uitbesteden van werkzaamheden, de eigenlijke dienstverlening, wordt meestal in een aparte overeenkomst geregeld.
[31] De ICT-dienstverlener kan dit uiteraard op een andere organisatorische wijze hebben ingericht.

24. Jaarlijks dient de beoordeling plaats te vinden, in opdracht van de systeem-, gegevens-, of proceseigenaar, door een onafhankelijke partij, die gespecialiseerd is in informatiebeveiliging.
25. Tussentijdse controles kunnen plaatsvinden door de interne accountantsdienst van de gemeente zelf. De bevindingen en verbeteringen zijn onderdeel van de jaarlijkse controle door de onafhankelijke partij.
26. Beoordeling vindt plaats op de volgende punten/onderdelen:
    - Of het beleid logische toegangsbeveiliging in overeenstemming is met de wet- en regelgeving en ander beleidsstukken.
    - Of de maatregelen passend zijn voor het beleid logische toegangsbeveiliging.
    - Of de gemeente in voldoende mate het beleid naleeft.

Aldus vastgesteld door burgemeester en wethouders van *[gemeente]* op *[datum],*

[Naam. Functie] [Naam. Functie]

_____ _____

Bijlage 2: Voorbeeld autorisatieprocedure tot <informatiesysteem>

Inleiding
De inhoud van deze autorisatieprocedure moet bekend zijn bij alle medewerkers die bij deze procedure betrokken zijn.

Doel
Deze autorisatieprocedure voorziet in het vastleggen van de verschillende stappen die noodzakelijk zijn voor het autoriseren van personen voor <informatiesysteem>. Hiermee wordt de logische toegangsbeveiliging geregeld voor de gegevens van <informatiesysteem> en de vertrouwelijkheid hiervan gewaarborgd.

Definitie
Met een autorisatie wordt een 'door het bevoegd gezag gelegitimeerde toegang' tot één of meerdere informatiesystemen van de gemeente bedoeld. De procedure bestaat uit drie afzonderlijke deelprocedures die gescheiden kunnen worden uitgevoerd:

- Autorisatie tot het netwerk
- Autorisatie tot <informatiesysteem>
- Periodieke controle autorisaties en rapportage

Verantwoordelijkheid
Voor elk bedrijfsproces, informatiesysteem, gegevensverzameling en ICT-faciliteit is een verantwoordelijke lijnmanager benoemd.

Beheer
Om toegang te kunnen krijgen tot de gegevens is naast de specifieke autorisatie in het desbetreffende informatiesysteem tevens een bevoegdheid nodig op netwerk- en/of systeemniveau. Deze bevoegdheden worden beheerd door de netwerk- en/of systeembeheerder. De bevoegdheden binnen <informatiesysteem> worden beheerd door de functioneel beheerder van <informatiesysteem>.

Proceseigenaar[32]
De proceseigenaar is de manager van de afdeling <afdeling>.

Verantwoordelijkheden
De verantwoordelijkheid voor deze autorisatieprocedure ligt bij het college van burgemeester en wethouders (college van B&W) en namens deze, bij de systeemeigenaar van het <informatiesysteem>. De systeemeigenaar stelt in overleg met de functioneel beheerder de autorisatiematrix op die als bijlage aan deze autorisatieprocedure wordt toegevoegd.
De verantwoordelijkheid om toegang te verlenen tot de gegevens behorend bij <informatiesysteem> berust bij de gegevenseigenaar. De uitvoering hiervan ligt bij de functioneel beheerder van <informatiesysteem>.

[32] Als het informatiesysteem meerdere processen ondersteunt zijn er meerdere proceseigenaren voor één informatiesysteem. Als dat het geval is dienen al deze proceseigenaren hier vermeld te worden.

Actualiteit
De systeemeigenaar is verantwoordelijk voor het actueel houden van deze autorisatieprocedure.

Autorisatie tot <informatiesysteem>

- De autorisatiebevoegde medewerker van <informatiesysteem> dient, met behulp van het daarvoor bestemde aanvraag- of wijzigingsformulier, schriftelijk een autorisatieverzoek in voor een nieuwe of gewijzigde autorisatie voor <informatiesysteem> bij de servicedesk.
- De servicedesk beoordeelt het autorisatieverzoek. Hierbij wordt gecontroleerd of het aanvraag- of wijzigingsformulier op de juiste manier is ingevuld en of het formulier door een autorisatiebevoegde medewerker is ingediend. Tevens wordt gecontroleerd of de aanvraag in overeenstemming is met de autorisatiematrix behorende bij <informatiesysteem>.
- De functioneel beheerder <informatiesysteem> die het bericht van de servicedesk ontvangt regelt vervolgens de autorisatie in <informatiesysteem>.
- De systemen zijn voor geautoriseerde gebruikers slechts toegankelijk met gebruik van persoonlijke toegangscodes (bijvoorbeeld wachtwoorden). Deze wachtwoorden dienen te voldoen aan de richtlijnen zoals vermeld in het wachtwoordbeleid van de gemeente.
- De servicedesk krijgt van de functioneel beheerder <informatiesysteem> die het autorisatieverzoek heeft verwerkt een terugmelding over het autorisatieverzoek. De servicedesk koppelt dit terug aan de gebruiker en tevens krijgt de gebruiker een korte instructie hoe deze zich aan kan melden en hoe om te gaan met <informatiesysteem>.
- Bij vertrek of wijziging van de functie van een medewerker geeft de verantwoordelijk manager van de medewerker dit door aan de servicedesk, waarna de functioneel beheerder de autorisatie intrekt of wijzigt.

Periodieke controle autorisaties en rapportage
De functioneel beheerder <informatiesysteem> zorgt minmaal één keer per kwartaal voor een overzicht van de in het informatiesysteem toegekende autorisaties. Mede op basis van dit overzicht controleert het management of de systeem-, gegevens-, of proceseigenaren of de toegangsrechten van medewerkers nog juist zijn binnen de informatiesystemen waar zij verantwoordelijk voor zijn, en brengt een rapportage uit aan de CISO.
In deze rapportage wordt aangegeven:

- Of de geïmplementeerde autorisaties overeenkomen met de toegekende autorisaties.
- Of de geregistreerde gebruikers en de aan hen toegekende autorisaties correct zijn. Hierbij wordt het controleverslag vergeleken met de autorisatieformulieren en tevens vergeleken met wat is vastgelegd in de autorisatiematrix <informatiesysteem>.
- Of bij tussentijdse wijzigingen in taak/functie de verantwoordelijke manager van de medewerker de servicedesk hierover informeert, en of bij ontslag of vertrek de autorisatie direct wordt geblokkeerd.

Indien de uitgevoerde controle hiertoe aanleiding geeft, geeft de CISO opdracht aan de functioneel beheerder <informatiesysteem>, om de nodige correcties aan te brengen. De functioneel beheerder <informatiesysteem> past zo nodig de autorisatie(s) aan en stelt de betreffende gebruiker op de hoogte van een wijziging in zijn bevoegdheidsprofiel.

Aldus vastgesteld door burgemeester en wethouders van *[gemeente]* op *[datum],*

[Naam. Functie] [Naam. Functie]

_____ _____

Bijlage 3: Voorbeeld procedure ontbreken voldoende functiescheiding

Inleiding
De inhoud van deze procedure moet bekend zijn bij alle medewerkers die bij deze procedure betrokken zijn. Deze procedure wordt alleen toegepast als niet voldaan kan worden aan de functiescheiding zoals de wet- en regelgeving[33] dit voorschrijft.

Doel
Doel van deze procedure is om bij het niet kunnen voldoen aan de vereiste functiescheiding toch de werkzaamheden, verband houdende met de <omschrijving uit te voeren activiteiten> te kunnen uitvoeren.

Definitie
Gelet op de personele bezetting van <aantal> personen op de afdeling <afdelingsnaam> is het niet mogelijk de vereiste functiescheiding (te allen tijde) door te voeren tussen de betrokken medewerkers bij <aangeven welke activiteiten het hier betreft>. Door het toepassen van deze procedure wordt aan de (wettelijke) verantwoordingsplicht voldaan.

Proceseigenaar
De proceseigenaar is de manager van de afdeling <afdeling>.

Verantwoordelijkheid
De verantwoordelijkheid voor deze autorisatieprocedure ligt bij het college van burgemeester en wethouders (college van B&W) en namens deze bij de systeemeigenaar van het <informatiesysteem>.

Actualiteit
De systeemeigenaar is verantwoordelijk voor het actueel houden van deze autorisatieprocedure.

Uitvoering[34]
Gedurende de periode, dat zich de hier bovenstaande situatie voordoet (of wanneer dit continu het geval is: minimaal eenmaal per kwartaal) wordt bijgehouden, wie de medewerkers zijn die in deze periode belast zijn met de aanvraag, de controle, het toekennen en het doorvoeren van de autorisaties. Tevens wordt schriftelijk vastgelegd wat de reden is waarom (tijdelijk) niet aan de eis van functiescheiding kan worden voldaan, en de periode waarin niet aan de eis van functiescheiding kan worden voldaan.
De betreffende aanvraagformulieren en de gegevens over de in deze periode verstrekte documenten worden afzonderlijk bewaard.

Periodieke controle autorisaties en rapportage

[33] Bijvoorbeeld zoals in artikel 93 van de Paspoortuitvoeringsregeling Nederland (PUN) (http://wetten.overheid.nl/BWBR0012811) en artikel 128 in het Reglement Rijbewijzen (http://wetten.overheid.nl/BWBR0008074/)
[34] Hierbij dient nog wel een controle te worden uitgevoerd of de hier vermelde schriftelijke vastlegging (uitvoering) voldoende is om te voldoen aan de specifieke artikelen die functiescheiding vereisen. Zoals artikel 93, lid 3 van de PUN en artikel 128, lid 3 van het Reglement Rijbewijzen..

De functioneel beheerder <informatiesysteem> zorgt direct of zo snel mogelijk na de bewuste periode of in ieder geval minimaal één keer per kwartaal voor een overzicht van de in het informatiesysteem toegekende autorisaties. Mede op basis van dit overzicht controleert het management of de toegangsrechten van medewerkers nog juist zijn binnen de informatiesystemen waar zij verantwoordelijk voor zijn en brengt een rapportage uit aan de CISO.

De controle richt zich vooral op:

- Het ontbreken van de vereiste functiescheiding.
- Of in de betreffende periode bijgehouden is wie de medewerker(s) is/zijn die in deze periode betrokken is/zijn geweest met de aanvraag, de controle, het toekennen en het doorvoeren van de autorisaties.
- Of de schriftelijke vastlegging aanwezig is en de aanvraag, controle, toekenning en het beheer op de voorgeschreven wijze hebben plaatsgevonden.

Aldus vastgesteld door burgemeester en wethouders van *[gemeente]* op *[datum],*

[Naam. Functie] [Naam. Functie]

_____ _____

Bijlage 4: Voorbeeld overzicht van informatiesystemen

Gemeenten dienen een actueel inzicht te hebben welke informatiesystemen binnen de gemeente worden gebruikt. Op het moment dat de gemeente beschikt over een configuratiebeheersysteem (CMDB)[35], dan zijn deze gegevens in deze CMDB vastgelegd en hoeft geen afzonderlijk overzicht te worden bijgehouden. Een informatiesysteem kan maar één systeemeigenaar hebben, maar een medewerker kan wel eigenaar zijn van meerdere informatiesystemen.

Informatiesysteem	Eigenaar	Configuratie-item
<informatiesysteem 1>	<eigenaar 1>	<informatiesysteem 1>
<informatiesysteem 2>	<eigenaar 2>	<informatiesysteem 2>
<informatiesysteem 3>	<eigenaar 1>	<informatiesysteem 3>
<informatiesysteem 4>	<eigenaar 4>	<informatiesysteem 4>
<informatiesysteem 5>	<eigenaar 1>	<informatiesysteem 5>
<informatiesysteem 6>	<eigenaar 6>	<informatiesysteem 6>

Informatiesysteem: De naam van het informatiesysteem, waar mogelijk aangevuld met versienummers.
Eigenaar: De systeemeigenaar van het informatiesysteem. Verschillende informatiesystemen kunnen dezelfde eigenaar hebben.
Configuratie-item: De unieke identificatiecode van het informatiesysteem zoals deze is geregistreerd in een configuratieregistratie binnen het configuratiebeheersysteem.

[35] Een gegevensbestand dat wordt gebruikt om de configuratieregistraties op te slaan tijdens hun levenscyclus. Het configuratiebeheersysteem slaat attributen van configuratie-items op. Evenals relaties met andere configuratie-items. De Engelse benaming is configuration management database (CMDB).

Bijlage 5: Voorbeeld autorisatieoverzichten

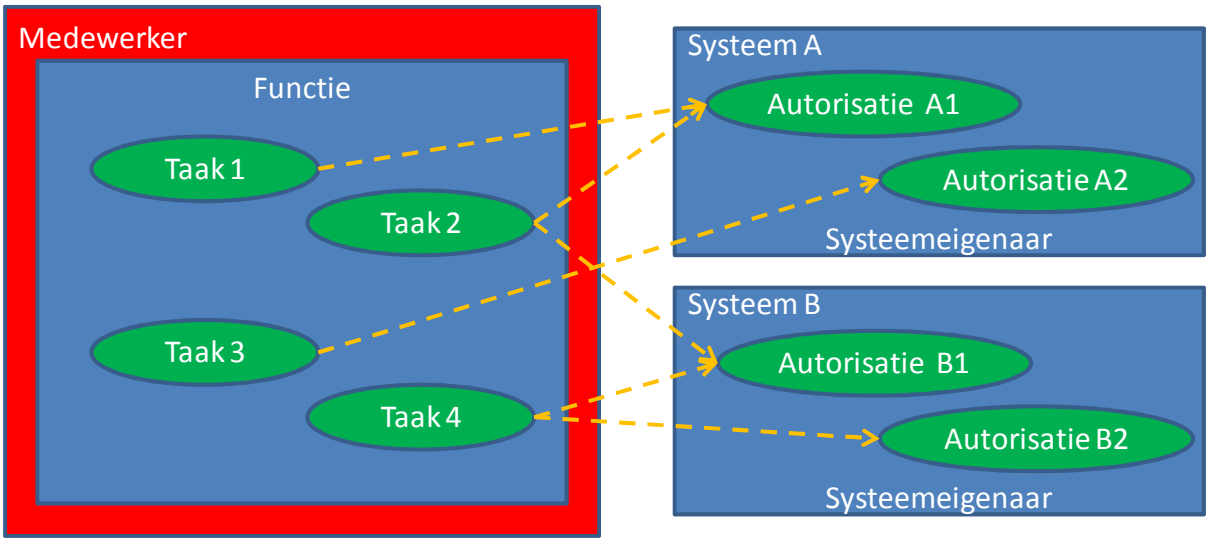
Gemeenten dienen een actueel inzicht te hebben wie, welke autorisaties heeft binnen de informatiesystemen die bij de gemeente worden gebruikt. Als gemeenten moet je daarvoor onderstaande vragen kunnen beantwoorden:

- Welke functies[36] binnen de gemeenten worden onderkend?
- Welke taken bij een specifieke functie horen?
- Welke taken niet gecombineerd mogen worden vanuit het oogpunt functiescheiding?
- Welke functie een medewerker bekleed?
- Welke taken een medewerker vervuld?

In figuur 3 wordt de relatie weergeven tussen de functie die een medewerker bekleedt, de taken die bij deze functie horen en de benodigde autorisaties die deze medewerker in de verschillende systemen moet hebben om deze taken te kunnen uitvoeren.

Bijvoorbeeld:

- Voor het uitvoeren van 'taak 1' heeft deze medewerker autorisatie A1 voor systeem A nodig.
- Voor het uitvoeren van 'taak 2' heeft deze medewerker autorisatie A1 voor systeem A en Autorisatie B1 voor systeem B nodig.
- Voor het uitvoeren van 'taak 3' heeft deze medewerker autorisatie A2 voor systeem A nodig.
- Voor het uitvoeren van 'taak 4' heeft deze medewerker autorisatie B1 en B2 voor systeem B nodig.



Figuur 3. Relatie Functie, taken en autorisaties

Gemeenten moeten inzicht hebben in welke taken behoren bij een specifieke functie. Hiervoor kan gebruik worden gemaakt van tabel 2. Deze verschillende taken kunnen betrekking hebben op verschillende informatiesystemen. Voorbeelden van functies zijn:

- Controller

[36] Een functie is een verzameling van taken, rechten en plichten voor een persoon binnen een bepaald domein, bijvoorbeeld binnen een bedrijf, vereniging, gemeente of project. In dit document wordt een functie gezien als het geheel van activiteiten, die als een logische eenheid van werk aan een medewerker kan worden toegewezen.

- Junior/senior inkoper
- Medewerker salarisadministratie
- Kwaliteitsmedewerker
- Lijnmanager
- Teammanager

Voorbeelden van taken zijn:

- Aanvragen bestellingen
- Accorderen bestellingen
- Invoeren betalingen
- Accorderen betalingen

X = Taak behorende bij functie	Taak 1	Taak 2	Taak 3	Taak 4	Taak 5	Taak 6	Taak 7
Functie 1		X					
Functie 2	X			X			
Functie 3				X	X		
Functie 4		X	X				
Functie 5			X				
Functie 6							
Functie 7							

Tabel 2. Overzicht welke taken behoren bij een specifieke functie

Gemeenten moeten inzicht hebben welke combinaties van taken (autorisaties binnen een informatiesysteem), wel en niet mogen worden toegekend aan één functie (medewerker). Hiervoor kan gebruik worden gemaakt van tabel 3. In dit overzicht dienen de functies voor te komen die uit het oogpunt van functiescheiding belangrijk zijn.
Autorisaties waarmee het informatiesysteem alleen geraadpleegd kan worden (rapporten afdrukken, schermen bekijken) mogen met andere autorisaties worden gecombineerd.

X = niet toegestane combinatie van autorisaties Bijvoorbeeld: Op het snijpunt van de regel taak 1 en de kolom taak 2 staat een X. Dat betekent dat een medewerker niet mag worden geautoriseerd voor deze beide rollen tegelijk.	Taak 1	Taak 2	Taak 3	Taak 4	Taak 5	Taak 6	Taak 7
Taak 1		X					
Taak 2	X			X			
Taak 3				X	X		
Taak 4		X	X				
Taak 5			X				
Taak 6							
Taak 7							

Tabel 3. Overzicht van wel en niet toegestane combinaties van taken

Gemeenten moeten inzicht hebben welke functie door één medewerker wordt ingevuld. Hiervoor kan gebruik worden gemaakt van tabel 4.

X = Functie die door de medewerker wordt ingevuld	Functie 1	Functie 2	Functie 3	Functie 4	Functie 5	Functie 6	Functie 7
Medewerker 1	X			X			
Medewerker 2			X	X			
Medewerker 3							X
Medewerker 4	X					X	
Medewerker 5			X				
Medewerker 6		X			X	X	
Medewerker 7							

Tabel 4. Overzicht welke functies worden uitgevoerd door een medewerker (autorisatiematrix)

Bijlage 6: Voorbeeld autorisatie aanvraagformulier <informatiesysteem>

Gegevens gebruiker		
Naam en voorletters gebruiker	<Volledige naam van de te autoriseren medewerker.>	
Voornaam gebruiker	<Voornaam van de te autoriseren medewerker.>	
E-mailadres	<E-mailadres van de te autoriseren medewerker.>	
Afdeling/Groep	<Organisatorische eenheid waarbij de te autoriseren medewerker werkzaam is.>	
Functie	<De functie van de te autoriseren medewerker.>	
Kamernummer	<Kamer waar de te autoriseren medewerker zijn vaste werkplek heeft. Dit veld kan leeg worden gelaten op het moment dat met flexibele werkplekken wordt gewerkt.>	
Telefoonnummer	<Telefoonnummer van de te autoriseren medewerker. Bij calamiteiten moet de verwerkingsorganisatie direct contact op kunnen nemen met de gebruiker. Tevens kan de medewerker bij een spoed autorisatie direct op de hoogte worden gesteld dat de autorisatie is toegekend.>	
Dienstverband (Tijdelijk/Vast)[37]	Tijdelijk / Vast[38]	
Autorisatie[39]	**Nieuwe gebruiker**	O
	Wijzig huidige autorisaties	O
	Opschorten gebruiker-ID	O
	Intrekken gebruiker-ID	O
Gebruiker-ID	<Als het een bestaande gebruiker betreft dient hier het huidige gebruikers-ID ingevuld te worden, bij een nieuwe gebruiker wordt dit door de verwerkingsorganisatie later ingevuld. Nieuwe gebruikers krijgen meestal een gebruikersnaam die van hun eigen naam is afgeleid. Deze gebruikersnaam wordt in het vakjargon gebruikers-ID genoemd.>	
Reden	<De reden van deze aanvraag/wijziging met betrekking tot de autorisaties van deze medewerker.>	
Gewenste ingangsdatum	<De datum waarop de autorisatie ingaat kan afwijken van de aanmelddatum maar moet daarna liggen. Het is aan te raden om de autorisaties ruim van te voren aan te melden zodat de werkzaamheden die bij het autoriseren horen kunnen worden ingepland.>	
Einddatum geldigheid[40]	<In veel gevallen zal deze rubriek leeg worden gelaten omdat er een permanente autorisatie wordt toegekend. Het komt echter voor dat bepaalde werkzaamheden slechts van korte	

[37] Bij tijdelijke medewerkers wordt, in tegenstelling tot vaste medewerkers, de autorisatie voor een bepaalde periode toegekend. Zie ook invoerveld 'Einddatum geldigheid'.
[38] Doorhalen wat niet van toepassing is.
[39] De aard van de autorisatie dient hier te worden aangegeven. Denk hierbij aan aanvragen, wijzigen, opschorten of intrekken. Aankruisen wat van toepassing is.
[40] Dit veld moet worden ingevuld op het moment dat het om een tijdelijk dienstverband gaat.

	duur zijn, medewerkers op contract worden aangenomen of vakantiewerk komen verrichten. In die gevallen wordt de 'Einddatum geldigheid' toegepast.>

Autorisaties <informatiesysteem>			
Vul de huidige, de gewenste en de te verwijderen autorisatierollen in[41]	**Huidige**	**Verwijderen**	**Nieuwe rol / Toevoegen**
<Rol 1>	O	O	O
<Rol 2>	O	O	O
<Rol 3>	O	O	O
Alle autorisaties verwijderen	O		

Gegevens Aanvrager[42]	
Naam en voorletters aanvrager	<Volledige naam van de autorisatiebevoegde medewerker.>
Voornaam aanvrager	<Voornaam van de autorisatiebevoegde medewerker.>
Telefoonnummer	<Telefoonnummer van de autorisatiebevoegde medewerker.>
E-mailadres	<E-mailadres van de autorisatiebevoegde medewerker.>
Functie	<De functie van de autorisatiebevoegde medewerker dient tevens ter verificatie te worden vermeld zodat wordt voorkomen dat de aanvrager autorisaties uitgeeft van informatiesystemen waarvoor hij niet geautoriseerd is.>
Aanmelddatum	<Datum waarop de autorisatie is aangevraagd. Aan de hand van deze datum kan achteraf worden vastgesteld hoe lang het heeft geduurd voordat de autorisatie werd ingevoerd.>
Handtekening[43]	<Handtekening van de autorisatiebevoegde medewerker. Deze handtekening dient op juistheid te worden gecontroleerd aan de hand van de parafen lijst.>

[41] Aankruisen wat van toepassing is.
[42] De aanvragen is niet de medewerker die de autorisatie krijgt, maar de medewerker die de autorisatie voor hem aanvraagt. Meestal is dit een lijnfunctionaris die hiervoor zelf is geautoriseerd.
[43] Autorisatieverzoeken worden uitsluitend in behandeling genomen indien deze zijn ondertekend door een daartoe bevoegd persoon (IV).

Bijlage 7: Literatuur/bronnen

Voor deze publicatie is gebruik gemaakt van onderstaande bronnen:

Titel: Werkprogramma logische toegangsbeveiliging
Datum: 16 juni 2005
Wie: EDP Audit Pool[44]

Titel: Methoden en technieken voor logische toegangsbeveiliging
Datum: oktober 2001
Wie: Praktijkgids De Controller & Informatiemanagement afl. 33 (ing. E. Beijer RE)
Link: http://www.finance-control.nl/artikel/6804/Methoden-en-technieken-voor-logische-toegangsbeveiliging

[44] De Rijksauditdienst (RAD) bundelt de krachten van de voormalige departementale auditdiensten van BZK, Financiën, VROM en VWS, de EDP Audit Pool en de afdeling Auditbeleid van de directie Coördinatie Auditbeleid Departementen. De Rijksauditdienst (RAD) is opgegaan in de Auditdienst Rijk (ADR) http://www.rijksoverheid.nl/onderwerpen/rijksoverheid/bedrijfsvoering-van-het-rijk/auditbeleid/auditdiensten

INFORMATIE BEVEILIGINGS DIENST

**INFORMATIEBEVEILIGINGSDIENST
V00R GEMEENTEN (IBD)**

**NASSAULAAN 12
2514 JS DEN HAAG**

**POSTBUS 30435
2500 GK DEN HAAG**

**HELPDESK 070 373 80 11
ALGEMEEN 070 373 80 08
FAX 070 363 56 82**

**IBD@KINGGEMEENTEN.NL
WWW.KINGGEMEENTEN.NL**

KWALITEITSINSTITUUT NEDERLANDSE GEMEENTEN **IN OPDRACHT VAN**
VERENIGING VAN NEDERLANDSE GEMEENTEN