


Doc. PL-8.2	Titel: Speciale Toegangsrechten	provincie limburg 
Classificatie: Bedrijfsvertrouwelijk	Datum: 01/06/2026	
Auteur: [REDACTED] Document status : Vaststelling MT	Versie: 1.0 Pag:1	

1 Inleiding

Dit hoofdstuk beschrijft de speciale toegangsrechten voor de beheerders die zijn ondergebracht binnen I-services. De beheerdersgroep bestaat uit de volgende afdelingen:

1. Helpdesk (HD)
2. Functioneel Beheer (FB)
3. Technisch Beheer (TB);
 - a. Technisch Applicatie Beheer (TAB)
 - b. Technisch Infrastructuur Beheer (TIB)

Voor het beheer van systemen en toepassingen zijn speciale rechten vereist. Het betreft onder andere rechten om gebruikers toegang te verlenen en om controles in te stellen of juist op te heffen. Ongepast gebruik van deze speciale rechten voor systeem-, netwerk en applicatiebeheer is een factor die in grote mate bijdraagt aan bijvoorbeeld storingen in informatie verwerkende systemen of ongeautoriseerde toegang tot informatie. Daarom zijn er aanvullende beveiligingsmaatregelen vereist voor het gebruik van deze speciale rechten.

LEGENDA:


De opbouw is als volgt:

- *Blauwe cursieve tekst bevat de relevante ISO2700x norm.*
- *Groene tekst geeft de control uit de BIO weer*
- *Gele tekst geeft de control uit de DIGID weer*
- *Rode tekst geeft de control uit de AVG weer*
- *Zwarte tekst geeft de feitelijke inhoud weer.*

Versiebeheer

Versie	Datum	Wie	Wat
0.1	2024	[REDACTED]	Initiële opzet document
1.0	14-4-2025	[REDACTED]	Verwerken feedback

[REDACTED]
[REDACTED]

Doc. PL-8.2	Titel: Speciale Toegangsrechten	provincie limburg 
Classificatie: Bedrijfsvertrouwelijk	Datum: 01/06/2026	
Auteur: [REDACTED] Document status : Vaststelling MT	Versie: 1.0 Pag:2	

2 Managementsamenvatting

Interne verhoogde toegangsrechten

Gebruikers met speciale toegangsrechten, ook wel de “Beheerders” is een speciale groep binnen de Provincie Limburg. De beheerdersgroep bestaat uit de volgende afdelingen:

1. Helpdesk (HD)
2. Functioneel Beheer (FB)
3. Technisch Beheer (TB);
 - a. Technisch Applicatie Beheer (TAB)
 - b. Technisch Infrastructuur Beheer (TIB)

Een indicatie van de functiescheiding op basis van toegangsrechten is hieronder globaal weergegeven:

	KLM-schijven	Active Directory	Applicaties	Databases	Servers	Netwerkkapparatuur
HD	■	■	■	■	■	■
FB	■	■	■	■	■	■
TAB	■	■	■	■	■	■
TIB	■	■	■	■	■	■

[REDACTED]
[REDACTED]
[REDACTED]


Speciale toegangsrechten vervallen zodra de betreffende beheerder de omschreven functietitel niet meer uitvoert. Ook bij een (tijdelijke) functieverandering worden de toegangsrechten per direct ontnomen.

Het beheerdersaccount heeft verhoogde rechten. Dit account wordt gebruikt op een zogeheten “beheercomputer” die in een speciaal netwerksegment zit. Dit account heeft een afwijkende benaming ten opzichte van de reguliere accounts.

Halfjaarlijks worden de toegangsrechten van beheerders beoordeeld. De Teamleider I-services beoordeeld dan o.a. wie een beheerder is en tot welke groepen (en daarmee applicaties of IT-componenten) de beheerder toegang heeft.

Externe verhoogde toegangsrechten

Externen met verhoogde toegangsrechten loggen in via de [REDACTED]. Deze dient verplicht beveiligd te worden met [REDACTED]. Hierdoor kan de externe het account niet delen met derden. Tot slot staan externe accounts standaard [REDACTED] verzoek van een interne contactpersoon.

Doc. PL-8.2	Titel: Speciale Toegangsrechten		provincie limburg 
Classificatie: Bedrijfsvertrouwelijk		Datum: 01/06/2026	
Auteur: [REDACTED]		Versie: 1.0	
Document status : Vaststelling MT		Pag:3	

3 Normtekst

8.2 Speciale toegangsrechten

Beheersmaatregel

Het toewijzen en gebruik van speciale toegangsrechten behoren te worden beperkt en beheerd.


Doel

Bewerkstelligen dat alleen bevoegde gebruikers, softwarecomponenten en diensten speciale toegangsrechten krijgen.

Richtlijn

Het toewijzen van speciale toegangsrechten behoort te worden beheerst door een autorisatieprocedure die in overeenstemming is met het relevante onderwerpspecifieke beleid inzake toegangsbeveiliging (zie 5.15). Het volgende behoort te worden overwogen:

- a) *het identificeren van gebruikers die speciale toegangsrechten nodig hebben voor elk systeem of proces (bijv. besturingssystemen, databasebeheersystemen en toepassingen);*
- b) *het toekennen van speciale toegangsrechten aan gebruikers waar nodig en van gebeurtenis tot gebeurtenis, overeenkomstig het onderwerpspecifieke beleid inzake toegangsbeveiliging (zie 5.15) (d.w.z. alleen aan personen met de nodige competentie om de activiteiten uit te voeren die speciale toegang vereisen en op basis van de minimumeisen voor hun functionele rol);*
- c) *een autorisatieproces in stand houden (d.w.z. bepalen wie speciale toegangsrechten kan goedkeuren, of speciale toegangsrechten pas toekennen als het autorisatieproces is afgerond) en een registratie van alle toegewezen rechten bijhouden;*
- d) *het definiëren en implementeren van eisen voor het vervallen van speciale toegangsrechten;*
- e) *het treffen van maatregelen om te bewerkstelligen dat de gebruikers zich bewust zijn van hun sp*
[REDACTED]
[REDACTED]
[REDACTED];
- f) *de authenticatie-eisen voor speciale toegangsrechten kunnen hoger zijn dan de eisen voor normale toegangsrechten. Herauthenticeren of het aanscherpen van het authenticeren kan nodig zijn voordat er werk met speciale toegangsrechten kan worden uitgevoerd;*
- g) *het regelmatig en na elke organisatiewijziging beoordelen van de gebruikers die met speciale toegangsrechten werken om te verifiëren of ze op grond van hun taken, rollen, verantwoordelijkheden en competentie nog altijd in aanmerking komen voor het werken met speciale toegangsrechten (zie 5.18);*
- h) *het vaststellen van specifieke regels om het gebruik van generieke gebruikersidentificaties voor beheer (zoals 'root') te vermijden, afhankelijk van de configuratiemogelijkheden van de systemen. Het beheren en beschermen van de authenticatie-informatie van dergelijke identiteiten (zie 5.17);*
- i) *tijdelijke speciale toegangsrechten slechts verlenen voor het tijdsvenster dat nodig is om goedgekeurde veranderingen of activiteiten te implementeren (bijv. voor onderhoudsactiviteiten of bepaalde essentiële veranderingen), in plaats van speciale toegangsrechten permanent te verlenen. Dit wordt vaak aangeduid als een procedure voor noodtoegang, en wordt vaak geautomatiseerd door technologieën voor het beheer van speciale toegangsrechten;*
- j) *het registreren van alle speciale toegang tot systemen voor auditdoeleinden;*

Doc. PL-8.2	Titel: Speciale Toegangsrechten	<div> <div>provincie limburg</div>  </div>
Classificatie: Bedrijfsvertrouwelijk	Datum: 01/06/2026	
Auteur: [REDACTED]	Versie: 1.0 Pag:4	

k) *identiteiten met speciale toegangsrechten niet met meerdere personen delen of aan meerdere personen koppelen, maar aan elke persoon een afzonderlijke identiteit toekennen waarmee specifieke speciale toegangsrechten kunnen worden toegekend. Identiteiten kunnen worden gegroepeerd (bijv. door een beheedersgroep te definiëren) om het beheer van speciale toegangsrechten te vereenvoudigen;*

l) *het gebruik van identiteiten met speciale toegangsrechten beperken tot het uitvoeren van beheerfuncties en deze identiteiten niet gebruiken voor de dagelijkse algemene taken [d.w.z. e-mail bekijken, toegang tot internet (gebruikers behoren voor deze activiteiten een afzonderlijke normale netwerkidentiteit te hebben)].*


Overige informatie

Speciale toegangsrechten zijn toegangsrechten die aan een identiteit, rol of proces worden verleend om activiteiten te kunnen uitvoeren die gewone gebruikers of processen niet kunnen uitvoeren.

Systeembeheerdersrollen vereisen meestal speciale toegangsrechten.

Ongepast gebruik van speciale systeembeheerdersrechten (elke functie of faciliteit van een informatiesysteem die de gebruiker in staat stelt systeem- of toepassingsbeheersmaatregelen op te heffen) is een factor die in grote mate bijdraagt aan storingen van of inbreuken op het systeem.


Meer informatie over toegangsbeheer en het beveiligde beheer van de toegang tot informatie en informatie- en communicatiemiddelen is te vinden in ISO/IEC 29146.

Doc. PL-8.2	Titel: Speciale Toegangsrechten	provincie limburg 
Classificatie: Bedrijfsvertrouwelijk	Datum: 01/06/2026	
Auteur: XXXXXXXXXX	Versie: 1.0 Pag:5	

4 Beschreven maatregelen

Inhoud

1	Inleiding	1
	Versiebeheer	1
2	Managementsamenvatting	2
3	Normtekst.....	3
4	Beschreven maatregelen.....	5
5	Algemeen.....	6
5.1	Identificeren van gebruikers met speciale toegangsrechten	6
5.2	Toekennen van speciale toegangsrechten	7
5.3	Autorisatieproces	7
5.4	Vervallen van speciale toegangsrechten.....	7
5.5	Bewustwording speciale toegangsrechten	7
5.6	Authenticatie-eisen speciale toegangsrechten	7
5.7	Regelmatig beoordelen speciale toegangsrechten	7
5.8	Generieke gebruikersidentificaties	7
5.9	Tijdelijke speciale toegangsrechten toekennen	7
5.10	Registreren van speciale toegang tot systemen	8
5.11	Identiteiten met speciale toegang niet delen met meerdere personen.....	8
5.12	Identiteiten met speciale toegangsrechten beperken tot het uitvoeren van de beheersfuncties	8

Doc. PL-8.2	Titel: Speciale Toegangsrechten		provincie limburg 
Classificatie: Bedrijfsvertrouwelijk		Datum: 01/06/2026	
Auteur: [REDACTED]		Versie: 1.0	
Document status : Vaststelling MT		Pag:6	

5 Algemeen

Dit hoofdstuk is van toepassing op de speciale toegangsrechten van gebruikers.

5.1 Identificeren van gebruikers met speciale toegangsrechten

Gebruikers met speciale toegangsrechten, ook wel de “Beheerders” is een speciale groep binnen de Provincie Limburg. De beheerdersgroep bestaat uit de volgende afdelingen:

4. Helpdesk (HD)
5. Functioneel Beheer (FB)
6. Technisch Beheer (TB);
 - a. Technisch Applicatie Beheer (TAB)
 - b. Technisch Infrastructuur Beheer (TIB)

























De Helpdesk biedt eerstelijns ondersteuning en kan voor een beperkte groep accounts wachtwoorden resetten. Zij hebben bijvoorbeeld geen toegang tot servers en netwerkapparatuur.

Functioneel beheer doet de functionele inrichting van (cloud) applicaties. De rechten limiteren zich tot een beperkte set applicaties die bij een beheerder in het takenpakket aanwezig zijn.

Technisch applicatiebeheer zorgt dat applicaties de juiste configuratie hebben en tijdig geüpdatet worden. Ook het beheer van werkplekken (VDI's) en databases valt hieronder. Deze groep beheerders hebben beperkte toegangsrechten tot de infrastructuur zoals servers en databases.


Technisch Infrastructuurbeheer beheert het kloppend hart van de Provincie; de serverruimte. Denk hierbij aan servers, netwerkapparatuur en virtualisatiesoftware.

Een indicatie van de functiescheiding op basis van toegangsrechten is hieronder globaal weergegeven:

	KLM-schijven	Active Directory	Applicaties	Databases	Servers	Netwerkapparatuur
HD						
FB						
TAB						
TIB						

[REDACTED]
[REDACTED]
[REDACTED]

Accounts met verhoogde rechten hebben de volgende naamgeving [REDACTED] De [REDACTED] zijn de initialen van de betreffende beheerder.

Doc. PL-8.2	Titel: Speciale Toegangsrechten	<div> <div>provincie limburg</div>  </div>
Classificatie: Bedrijfsvertrouwelijk	Datum: 01/06/2026	
Auteur: [REDACTED] Document status : Vaststelling MT	Versie: 1.0 Pag:7	

5.2 Toekennen van speciale toegangsrechten

Het toekennen van speciale toegangsrechten vindt veelal centraal plaatst via de Active Directory (AD). Sommige systemen ondersteunen deze koppeling echter niet. Op deze systemen worden de toegangsrechten decentraal ingeregeld.

5.3 Autorisatieproces

Speciale toegangsrechten zoals hierboven beschreven worden alleen maar toegekend aan mensen met deze functie en/of rol. De aanvrager dient conform het mandaatregister mandaat te hebben om een dusdanige wijziging in toegangsrechten aan te vragen.

5.4 Vervallen van speciale toegangsrechten

Speciale toegangsrechten vervallen zodra de betreffende beheerder de omschreven functietitel niet meer uitvoert. Ook bij een (tijdelijke) functieverandering worden de toegangsrechten per direct ontnomen.

5.5 Bewustwording speciale toegangsrechten

Beheerders hebben twee accounts;

Account 1 is het normale account zoals iedere ambtenaar heeft; Hierop vinden de dagelijkse werkzaamheden plaats zoals het e-mailen en verwerken van documenten.

Account 2 is het speciale beheerdersaccount. Dit account wordt gebruikt op een zogeheten "beheercomputer" die in een speciaal netwerksegment zit. Dit account heeft een afwijkende benaming ten opzichte van de reguliere accounts.

5.6 Authenticatie-eisen speciale toegangsrechten

De beheerderaccounts zijn voorzien van multifactor authenticatie.

5.7 Regelmatig beoordelen speciale toegangsrechten


Halfjaarlijks worden de toegangsrechten van beheerders beoordeeld. De Teamleider I-services beoordeeld dan o.a. wie een beheerder is en tot welke groepen (en daarmee applicaties of IT-componenten) de beheerder toegang heeft.

5.8 Generieke gebruikersidentificaties

De Provincie Limburg hanteert het beleid dat geen generieke gebruikersidentificaties aangemaakt worden, tenzij deze herleidbaar zijn tot een natuurlijkpersoon door middel van logging.

5.9 Tijdelijke speciale toegangsrechten toekennen

Medewerkers die tijdelijk in dienst zijn worden ook als zodanig opgevoerd in [REDACTED] Active Directory. De uit dienst datum van het betreffende account is automatisch gekoppeld aan [REDACTED]. Dit betekent dat wanneer het contract verloopt, het account automatisch dicht gezet wordt. Dit principe geldt ook voor accounts met verhoogde privileges. Voor externe leveranciers geldt dat de accounts persoonsgebonden zijn en elk jaar de noodzaak geëvalueerd wordt. Ook staan deze externe accounts standaard dicht. De externe dient bij de contactpersoon een verzoek in te dienen.

Doc. PL-8.2	Titel: Speciale Toegangsrechten	provincie limburg 
Classificatie: Bedrijfsvertrouwelijk	Datum: 01/06/2026	
Auteur: XXXXXXXXXX	Versie: 1.0 Pag:8	
Document status : Vaststelling MT		

De contactpersoon meldt dit daarna bij de Helpdesk met een verzoek tot openstelling van het account.

5.10 Registreren van speciale toegang tot systemen

Accounts met (verhoogde) toegangsrechten zijn ten alle tijden herleidbaar naar een natuurlijk persoon door middel van logging. Voor externe accounts geldt dat dit wordt gelogd door de PAM-tooling. Ook worden tekstuele en visuele logging vastgelegd zodat de handelingen herleidbaar zijn.

5.11 Identiteiten met speciale toegang niet delen met meerdere personen

Voor externen met verhoogde rechten geldt dat deze accounts zijn gekoppeld met de zakelijk bedrijfstelefoon. Inloggen kan alleen door met de gekoppelde telefoon een QR-code te scannen. Het uitwisselen van gebruikersnaam en wachtwoord is daardoor vermoeilijkt. Daarbij is voor externe ingesteld dat een vorm van biometrische authenticatie noodzakelijk is. Aangezien dit uniek is voor ieder persoon, kan het account niet gedeeld worden.

5.12 Identiteiten met speciale toegangsrechten beperken tot het uitvoeren van de beheersfuncties

Zie 5.5 Bewustwording speciale toegangsrechten.