



Is ook gepubliceerd als bijlage binnen het beleid informatiebeveiliging Provincie Limburg:
https://www.limburg.nl/publish/pages/133/beleid_informatiebeveiliging_provincie_limburg_1.pdf

Beleid logische toegang Provincie Limburg

1. Beleidsuitgangspunten Provincie Limburg

Ten behoeve van de autorisatie voor de toegang tot applicaties en gegevens zijn in het kader van informatiebeveiliging een aantal beleidsuitgangspunten opgesteld. Het doel van dit beleid is te voorkomen dat onrechtmatig toegang verkregen wordt tot applicaties en gegevens van de Provincie Limburg. Het beleid logische toegangsbeveiliging is van toepassing op alle applicaties, gegevens en overige componenten van de informatievoorziening waarvan de Provincie Limburg eigenaar is. Dit geldt ook wanneer de informatievoorziening niet op de infrastructuur van de Provincie Limburg wordt uitgevoerd (hosting, cloud). Ook in die gevallen is het beleid logische toegang van toepassing.

2. Uitgangspunten logische toegang

De Provincie Limburg hanteert de volgende beleidsuitgangspunten en deze zijn mede ontleend aan de BIO:

Eigenaarschap

- Iedere applicatie en gegevensverzameling heeft een eigenaar;
- De eigenaar bepaalt de toegang tot de applicatie en de rechten binnen die applicatie;
- De eigenaar is verantwoordelijk voor adequate training in het gebruik van de applicatie;
- De eigenaar bepaalt wie toegang heeft tot gegevens uit de applicatie (voor zover dit al niet gebeurt op basis van applicatierechten);
- De eigenaar van een applicatie en gegevens 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 BIO of risicoanalyse voortvloeien;

Authenticatie

- Iedere persoon die gebruik maakt van de infrastructuur, applicaties en gegevens is bekend;
- Alleen personen die zijn opgenomen binnen het Personeelsinformatiesysteem van de Provincie Limburg (geverifieerde identiteit en screening) komen in aanmerking voor een account voor toegang tot de informatievoorziening van de Provincie Limburg;
- Authenticatie vanuit een onveilige zone¹ vindt plaats op basis van gebruikersnaam, wachtwoord en een tweede factor;

¹ Alleen het bekabelde netwerk binnen het gouvernement wordt gezien als veilige zone, Overige netwerken worden als onveilig beschouwd.



- Het verdient de voorkeur om in alle gevallen gebruik te maken van de generieke authenticatie methodiek;²
- Er worden in de regel geen 'algemene' (ongepersonaliseerde) identiteiten gebruikt.³

Wachtwoorden

- Het algemene wachtwoord sluit aan op de complexiteitsvoorschriften uit de BIO(9.4.3.1).
- Het wachtwoord heeft een geldigheid van maximaal 6 maanden;
- Applicaties die geen gebruik maken van de generieke authenticatie en autorisatie methodiek conformeren zich aan de standaard voor het wachtwoord;

Autorisatie

- Op basis van functie en rol van een medewerker worden autorisaties toegekend;
- De eigenaar van de applicatie en gegevens is verantwoordelijk voor een juiste toekenning en intrekking van de autorisatie;
- Autorisaties voor applicaties worden bij voorkeur beheerd vanuit een centrale omgeving;
- De eigenaar van een applicatie wordt periodiek (minimaal 1 maal per 6 maanden), ter beoordeling van de juistheid, op de hoogte gesteld van de betreffende autorisaties;

Functiescheiding

- De beschikkende, bewarende en controlerende taken worden in beginsel nooit bij één functionaris tezamen gebracht. Indien dit toch noodzakelijk is, dan worden voor de uitvoering van deze taken door de eigenaar van de applicatie aanvullende maatregelen genomen;
- Een autorisatie voor beheeractiviteiten dient zo veel als mogelijk gescheiden te zijn van autorisaties voor de gegevens binnen een dergelijk applicatie;

Privileged users

- Hieronder worden die interne en externe medewerkers verstaan die (tijdelijk) administrator-rechten hebben. Zij beschikken hiervoor over een persoonlijk admin-account;
- Het admin-account is toegekend aan één medewerker met de betreffende beheertaak;
- Een admin-account dient enkel gebruikt te worden bij de uitvoering van de betreffende administrator werkzaamheden. De hiervoor noodzakelijke rechten zijn toegekend aan dit account;
- Handelingen uitgevoerd met een admin-account worden gelogd;

Inhuur extern personeel

- De door Provincie Limburg ingehuurde externen vallen onverkort onder het beleid logische toegangsbeveiliging en dienen conform deze regels te handelen;
- Aan de hand van hun taken/functie/rol geeft de eigenaar van de applicatie ingehuurde externe medewerkers toegang tot de applicatie en de gegevens;

² Het gaat hier om de centrale registratie van identiteiten op basis van de gegevens uit het personeels informatie systeem en de koppeling hiervan aan "rollen" t.b.v. de autorisatie voor en binnen de verschillende applicaties

³ Uit A.9.2.1: "het gebruik van groepsidentificaties

behoort alleen te worden toegelaten als deze om bedrijfs- of operationele redenen noodzakelijk zijn en behoort te worden goedgekeurd en gedocumenteerd;"



Uitbestede dienstverlening

- De ICT-dienstverlener zal een beveiligingsbeleid moeten hebben en geëffectueerde maatregelen, die zij aan de Provincie Limburg inzichtelijk maakt en die in lijn zijn met dit beleid logische toegang;
- De ICT-dienstverlener is verantwoordelijk voor een correcte inrichting van het eigen beveiligingsbeleid en naleving hiervan binnen de eigen organisatie.
- De ICT-dienstverlener voldoet aan de normen en eisen die gesteld zijn in het informatiebeveiligingsbeleid c.q. beleid logische toegangsbeveiliging van de Provincie Limburg;
- De ICT-dienstverlener voldoet aan de van toepassing zijnde wet- en regelgeving;
-
- De ICT-dienstverlener beschikt over een functionaris informatiebeveiliging, die verantwoordelijk is voor het informatiebeveiligingsbeleid van de ICT-dienstverlener en die contactpersoon is voor de CISO van Provincie Limburg;
- De ICT-dienstverlener beschikt over een autorisatiebeheerder voor de dagelijkse operatie die verantwoordelijk is voor een correcte inrichting van de autorisaties en die op dit gebied aanspreekpunt is voor de systeem/gegevenseigenaar binnen de Provincie Limburg;
- De ICT-dienstverlener stelt capaciteit en informatie beschikbaar t.b.v. audits op het gebied van autorisaties, die in opdracht van Provincie Limburg uitgevoerd worden.

3. Controle en naleving

In lijn met het managementsysteem voor informatieveiligheid vindt rapportage plaats over de belangrijkste aspecten van authenticatie en autorisatie binnen de provincie.

4. Vaststelling

Dit beleidsdocument is vastgesteld door het directie team in de DT vergadering van dd. 4 juli 2022. Dit document wordt meegenomen in de jaarlijkse beoordeling van de beleidsdocumenten op het gebied van informatiebeveiliging.