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 provincie van belang dat zij tijdig over relevante en betrouwbare informatie beschikt. Om de informatiestromen te beheersen dient de provincie een proces in te richten dat bepaalt wie er wanneer toegang heeft tot informatie. Logische toegang is gebaseerd op de classificatie van informatie.

Doelstelling van logische toegangsbeveiliging is het vaststellen van de identiteit (authentiseren) van een gebruiker of een geautomatiseerd proces die toegang krijgt tot provinciale gegevens, informatiesystemen of diensten, en het waarborgen van een gecontroleerde toegang tot (autoriseren) en gebruik van provinciale gegevens, informatiesystemen of diensten door provinciemedewerkers en/of een derde partij tegen acceptabele kosten.

## Begrippenlijst

* **Beheerder technische Infrastructuur - deelgebied Technisch Beheer**De beheerder technische infrastructuur richt zich op het in stand houden, beheren en onderhoud van de IT-infrastructuur en heeft [ITIL](https://nl.wikipedia.org/wiki/ITIL) als standaard. De IT-infrastructuur is de basis waarop applicaties kunnen draaien en bestaat uit het netwerk, de computers (servers/clients), besturingssystemen en overige randapparatuur.
* **Technisch applicatiebeheerder/DBA - deelgebied Applicatiebeheer**Onder dit beheer wordt verstaan het in stand houden van de bedrijfsapplicaties en [gegevensverzamelingen](https://nl.wikipedia.org/wiki/Gegevensverzameling) (databases) van de organisatie. Hieronder valt bijvoorbeeld het inregelen en in stand houden van de hoge beschikbaarheid, schaalbaarheid en performance van de applicatie, het inregelen van de back-up van de data en herstel in geval van calamiteiten. Verder houdt de technisch applicatiebeheerder/DBA zich bezig met de creatie, beheer en wijzigen van applicaties en databases naar aanleiding van geconstateerde fouten of veranderende technische of functionele eisen. [ASL](https://nl.wikipedia.org/wiki/ASL-beheermethodiek) is hiervoor de standaard.
* **Technisch gegevensstructuurbeheerder – deelgebied Applicatiebeheer**
De gegevensstructuurbeheerder bepaalt in overleg met de functioneel en technisch applicatiebeheerder voor het betreffende informatiesysteem welke gegevens moeten worden opgeslagen en beheert de gegevensstructuur, het datamodel en over wie, wanneer, welke, gegevens mag aanmaken, bekijken, wijzigen en verwijderen (beveiliging incl. privacy).
* **Functioneel applicatie-eigenaar – deelgebied Functioneel beheer**Een functioneel applicatie-eigenaar is verantwoordelijk voor de functionaliteit van de applicatie. In veel gevallen is dit de lijnmanager van de afdeling waarin de functioneel applicatiebeheerder en materiedeskundigen van de betreffende applicatie zijn geplaatst.
* **Functioneel applicatiebeheerder – deelgebied Functioneel beheer**De functioneel applicatiebeheerder houdt zich bezig met het beheren van de informatievoorziening en het inhoudelijke inrichting en beheer van applicatie(s). De functioneel applicatiebeheerder is namens de gebruikersorganisatie verantwoordelijk voor de functionaliteit. De functioneel applicatiebeheerder is het contactpunt met de ICT afdeling of de externe ICT beheerder (leverancier). Hij of zij verzamelt de gebruikerseisen en wensen, prioriteert deze en zorgt voor aanpassing in de applicaties en test van deze aanpassingen voordat ze in productie worden genomen. De functioneel applicatiebeheerder zorgt dat de gebruikers goed kunnen werken met de applicatie; hij of zij zorgt voor opleiding, procedures, werkinstructies en minimaliseert risico’s door risico beperkende maatregelen.
* **Proceseigenaar – deelgebied Functioneel beheer**De proceseigenaar is verantwoordelijk voor de definitie van het proces, het onderhouden van die definitie, de bijbehorende hulpmiddelen en de ondersteunende materialen. Een proceseigenaar heeft de bevoegdheid om te bepalen hoe een proces verloopt. Deze persoon is ervoor verantwoordelijk dat het proces aan de verwachtingen van de organisatie voldoet en bijdraagt aan het behalen van de contractdoelstellingen.
* **Procesbeheerder – deelgebied Functioneel beheer**Een procesbeheerder legt het proces vast in nauwe afstemming met de proceseigenaar en beheert en documenteert het proces. Inhoudelijk heeft deze rol geen verantwoordelijkheid voor het proces zelf.
* **Functioneel gegevenseigenaar – deelgebied Functioneel beheer**Een gegevenseigenaar is verantwoordelijk voor de actualiteit en betrouwbaarheid van de vastgelegde gegevens. In veel gevallen is dit de lijnmanager van de afdeling waarin de functioneel beheerder en materiedeskundigen van de betreffende applicatie zijn geplaatst.
* **Functioneel gegevensbeheerder – deelgebied Functioneel beheer**De gegevensbeheerder draagt in opdracht van de gegevenseigenaar zorg voor een actueel en betrouwbaar gegevensbestand.

## Beleidsuitgangspunten

### Beleid voor toegangsbeveiliging (ISO 27001-A.9.1.1)

* Aan de hand van taken/functies wordt toegang verleend tot de gegevens en informatiesystemen. De proces-, applicatie en gegevenseigenaren zijn hiervoor verantwoordelijk. Zij stellen specifieke autorisatierollen op met de juiste rechten in afstemming met de functioneel applicatie- en gegevensbeheerder. Deze beheerders houden deze volgens een vastgestelde standaardprocedure bij.
	+ Het besturingssysteem moet door het vergelijken van de rol van de gebruiker met de vertrouwelijkheidsclassificatie[[1]](#footnote-1) van de gegevens ervoor zorgen dat de gebruiker de informatie mag verwerken.
	+ Er is geen toegang tot informatie mogelijk voordat er een vertrouwelijkheidsclassificatie aan is toegekend. Er moet een helder gedefinieerd toegangscontrolebeleid worden gevoerd.
	+ Het toegangscontrolebeleid bepaalt de toegangsrechten van iedere gebruiker (of groep gebruikers).
	+ Het toegangscontrolebeleid houdt rekening met het informatiebeleid m.b.t. informatieverstrekking (bijv. het 'intern openbaar, tenzij'-principe).
	+ Het toegangscontrolebeleid geldt ook voor informatiesystemen.
	+ Elke gegevensset heeft een eigenaar en deze moet op basis van wat de gebruiker vanuit zijn functie moet weten toegangsprofielen voor afzonderlijke gebruikers opstellen. De verantwoordelijkheid ligt bij de lijnmanager.
	+ De functioneel applicatie- en gegevensbeheerder (van transactieverwerkende systemen) regelt en documenteert in opdracht van de functioneel proces-, functioneel applicatie- en gevenseigenaar het toezicht op de uitvoering van de autorisatieprocedure.
	+ Voor systemen met een meer open karakter (bijv. sociale media, intranet) geldt dat gebruikers hun eigen verantwoordelijkheid moeten kennen en nemen.
* Toewijzing van rollen aan gebruikers dient de geautoriseerde werkzaamheden te weerspiegelen (op basis van functiescheiding).
* Iedere functioneel applicatie- en gegevensbeheerder zorgt voor een specifieke autorisatieprocedure voor elk informatiesysteem waarvan hij beheerder is en past deze toe. Hij hanteert daarbij de volgende uitgangspunten:
	1. De autorisatiestructuur van een informatiesysteem sluit aan bij de goedgekeurde procesbeschrijvingen.
	2. De functioneel applicatie- en gegevensbeheerder krijgt gegevens van de betrokken Proces-, applicatie- en gegevenseigenaren over de autorisatierollen en de daaraan gekoppelde gebruikersautorisaties.
	3. De functioneel applicatie- en gegevensbeheerder houdt rekening met mogelijk van toepassing zijnde wet- en regelgeving.
	4. Er worden in de regel geen ‘algemene’ (niet gepersonaliseerde) identiteiten gebruikt.
* Aan de hand van taken/functies wordt toegang verleend tot de gegevens en informatiesystemen. De functioneel applicatie- en gegevensbeheerder stelt hiervoor specifieke autorisatierollen op met de juiste rechten en houdt deze volgens een procedure bij.
	+ Het toegangscontrolemechanisme kan verschillende rapporten over de aan individuen toegewezen rechten weergeven.

### Toegang tot netwerken en netwerkdiensten (ISO 27001-A.9.1.2)

* Het logische toegangsbeleid is van toepassing op alle netwerkdiensten waarvan de provincie eigenaar is of formeel gebruik van maakt.
	+ Er zijn autorisatieprocedures opgesteld om te bepalen wie toegang tot welke netwerken en netwerkdiensten heeft.
	+ Er zijn beheersmechanismen en procedures opgesteld om de toegang tot netwerkverbindingen te beschermen.

### Registratie en afmelden van gebruikers (ISO 27001-A.9.2.1)

* Er wordt een register van gebruikers bijgehouden.
* Iedere gebruikersnaam behoort bij één persoon.
* De gebruikersnaam geeft geen indicatie van het privilegeniveau van de gebruiker, met uitzondering van de specifieke systeemgebonden accounts.

### Gebruikers toegang verlenen (ISO 27001-A.9.2.2)

* Voor elk bedrijfs- of werkproces, informatiesysteem, gegevensverzameling is een verantwoordelijke lijnmanager benoemd. Deze kan zijn verantwoordelijkheid toetsen aan richtlijnen:
* Er zijn beheerrichtlijnen voor het gemeenschappelijk gebruik van informatie.
* Er zijn richtlijnen om de categorieën van personeelsleden, contractanten en zakenpartners aan te geven, die de kantoorapplicaties mogen gebruiken.

### Beheren van speciale toegangsrechten (ISO 27001-A.9.2.3)

* Beheerders technische infrastructuur en technische applicatiebeheerders/DBA’s) mogen niet rechtstreeks in de database de data van het informatiesysteem muteren. Indien dit toch noodzakelijk is dan wordt elke handeling vastgelegd en er wordt door de proces-, functioneel applicatie- en gegevenseigenaar apart toezicht georganiseerd op de betreffende functionaris.
* Er zijn personeelscategorieën vastgesteld waaraan bijzondere rechten moeten worden toegekend.
* Er wordt een overzicht bijgehouden van alle toegekende bijzondere rechten.
* Er wordt een overzicht bijgehouden aan wie deze bijzondere rechten zijn toegekend.
* Alle handelingen moeten verantwoord kunnen worden.
* Alle pogingen om het logbestand met gebruikersactiviteiten te wissen, overschrijven of wijzigen moeten kunnen worden verantwoord.
* Beheer- en onderhoudshandelingen op systeemniveau worden waar mogelijk vastgelegd.
* We streven ernaar dat iedere geautoriseerde beheerder uniek geïdentificeerd kan worden.
* Voor extern personeel wordt voor het definiëren en toekennen van bevoegdheden een overeenkomstige procedure als voor het eigen personeel toegepast.
* Deze regel geldt tevens voor opsporingsambtenaren, indien zij in het kader van een justitieel onderzoek toegang verkrijgen tot persoonsgegevens.

### Scheiding van taken (ISO 27001-A.6.1.2)

* De beschikkende, bewarende, registrerende en controlerende taken worden in beginsel nooit in één functionaris tezamen gebracht. Indien dit toch noodzakelijk is dan wordt door de lijnmanager apart toezicht georganiseerd op de betreffende functionaris.
* Het toegangscontrolebeleid specificeert waar functiescheiding wordt toegepast.
* Verantwoordelijkheden zijn zodanig verdeeld dat geen enkele gebruiker met bijzondere rechten ongeautoriseerde handelingen kan verbergen.
* Gewaarborgd is, zowel in de organisatie als in de ICT infrastructuur, dat de toegekende bevoegdheden volledig en juist in het toegangscontrolesysteem zijn geïmplementeerd.

### Toegang tot persoonsgegevens en personeelsdossiers (ISO 27001-A.7.1.1)

* Niet-elektronische personeelsdossiers moeten achter slot en grendel worden bewaard.
* Het afdelingshoofd P&O geeft door middel van de aanwijzingsregeling aan welke functionarissen toegang tot de persoonsgegevens mogen hebben en welke functie(s) mogen worden uitgevoerd.
* Het afdelingshoofd P&O geeft door middel van de aanwijzingsregeling aan, wie in de organisatie bevoegdheden voor het verwerken van persoonsgegevens mag hebben.
* Tijdelijke medewerkers krijgen onder strikte, schriftelijk overeengekomen, voorwaarden toegang tot verwerkingen van persoonsgegevens.

### Bewustwording logisch toegangsbeheer (ISO 27001-A.7.2.2 en A.9.3.1)

* Gebruikers wordt bij indiensttreding geïnformeerd over de provinciale beveiligingsprotocollen en dienen deze in acht te nemen.
* Een medewerker, zowel vast als tijdelijk, intern of extern is verplicht te voorkomen dat onbevoegden toegang krijgen tot de systemen met informatie waar zij geen kennis van behoren te nemen dan wel dat informatie kan worden aangepast.
* Gebruikers dienen zich bewust te zijn van de verantwoordelijkheid om onjuist toegekende rechten onverwijld te melden aan de servicedesk.

### Beëindiging of wijziging van het dienstverband (ISO 27001-A.7.3.1 en A.9.2.6)

* Bij ontslag, vertrek, wijziging van functie of bij verlies van bevoegdheid om andere redenen, worden de bevoegdheden van de betrokken functionaris met onmiddellijke ingang ontnomen.
	+ Afdeling P&O dient onverwijld de diverse verantwoordelijke lijnmanagers in te lichten bij ontslag, vertrek, wijziging van functie (volgens de in- en uitdienstprocedure) zodat de toegangsrechten van betrokkene in de diverse systemen direct conform de standaardprocedure kunnen worden aangepast dan wel verwijderd teneinde misbruik van informatie te voorkomen.
	+ Oude en ongebruikte accounts worden verwijderd of gedeactiveerd.
	+ De toegangsrechten van mensen die een andere functie krijgen worden onmiddellijk gewijzigd.

### Systeemdocumentatie (ISO 27001-A.8.2.3)

* Toegang tot systeemdocumentatie moet door de proces-, functioneel applicatie-, gegevenseigenaar geautoriseerd worden.
* Systeemdocumentatie op informatiesystemen dient alleen toegankelijk voor geautoriseerd personeel te zijn.

## Afwijking van beleid

Indien noodgedwongen van dit beleid moet worden afgeweken, moeten de volgende stappen worden genomen:

1. Beschrijving en motivering van de afwijking vastleggen in een documentair informatie systeem;
2. Gedocumenteerde risicoanalyse uitvoeren en vastleggen in een documentair informatie systeem;
3. Voorleggen aan de proces-, functioneel applicatie- en gegevenseigena(a)r(en).
4. Proces-, functioneel applicatie- en gegevenseigena(a)r(en) dienen hiermee in te stemmen;
5. Kennisgeving aan de concerncontroller sturen;
6. Meenemen in de periodieke rapportage (zie 1.6).

## Rapportage en controle (ISO 27001-A.9.2.5)

* Minimaal eens per half jaar wordt gecontroleerd of toegangsrechten van medewerkers nog juist zijn. Per applicatie wordt dit door de functioneel applicatie- en gegevensbeheerder gerapporteerd aan de proces-, functioneel applicatie- en gegevenseigenaar. ~~Hierover vindt rapportage plaats naar het directieberaad.~~

Aldus vastgesteld door … op *[datum],*

[Naam. Functie] [Naam. Functie]

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. Vertrouwelijkheidsclassificaties bij Provincie Zeeland zijn: Extern openbaar, intern openbaar, vertrouwelijk en geheim. Het uitgangspunt is "Intern openbaar, tenzij". [↑](#footnote-ref-1)