B11 Autorisatiebeheer

<organisatie>

*Dit document is geldig tot: <datum>.*

*Classificatie: 3.*

Inhoudsopgave

[1 Versiebeheer 3](#_Toc83980868)

[2 Doel van dit document 4](#_Toc83980869)

[3 Reikwijdte en gebruikers 4](#_Toc83980870)

[3.1 Reikwijdte 4](#_Toc83980871)

[3.2 Gebruikers 4](#_Toc83980872)

[4 Gerelateerde documenten 4](#_Toc83980873)

[5 Voorwaarden 5](#_Toc83980874)

[6 Toegangsbeheer 5](#_Toc83980875)

[6.1 Principes en regels 5](#_Toc83980876)

[6.2 Uitgifte wachtwoorden 5](#_Toc83980877)

[6.3 Wachtwoordeisen 6](#_Toc83980878)

[7 Vaststellen doeltreffendheid 6](#_Toc83980879)

[7.1 Criteria 6](#_Toc83980880)

[7.2 Controles en registraties 6](#_Toc83980881)

[7.3 Administraties 6](#_Toc83980882)

# Versiebeheer

|  |  |  |  |
| --- | --- | --- | --- |
| **Versie** | **Auteur** | **Wijziging (omschrijving)** | **Datum vaststelling** |
| 1.0 |  | Initiatiedocument. |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# Doel van dit document

In dit document zijn de algemene regels en uitgangspunten vastgelegd met betrekking tot het geven/ontnemen en aanpassen van toegangsrechten tot informatie en informatiesystemen van <organisatie>.

Met dit document zorgt <organisatie> ervoor dat gebruikers de juiste toegangsrechten hebben in lijn met wetgeving en het ‘need to know’ principe.

# Reikwijdte en gebruikers

## Reikwijdte

De reikwijdte van dit document komt overeen met die van het *B01 Informatiebeveiligingsbeleid <organisatie>*.

## Gebruikers

De gebruikers van dit document zijn:

* Security Officer.
	+ Draagt als eigenaar zorg voor de correctheid van het document.
* Directie.
	+ Moet het document vaststellen.
* Eigenaren bedrijfsmiddelen.
	+ Moeten zich conformeren aan de regels zoals gesteld in het document.

# Gerelateerde documenten

Dit document heeft een relatie met documenten uit het ISMS van <organisatie>. B11 Autorisatiebeheer::

* Gebruikt de reikwijdte en doelstellingen zoals gegeven in **B01 Informatiebeveiligingsbeleid**.
* Wordt beheerst op de manier zoals beschreven in **B02 Documentbeheer ISMS**.
* Levert input op de gedragsregels die weergegeven staan in het **Communicatieblad regels informatiebeveiliging**.
* Gebruikt de resultaten van de afhankelijkheidsanalyse zoals gegeven in **overzicht afhankelijkheden bedrijfsmiddelen**.
* Leidt tot de noodzaak informatiebeveiligingsincidenten te melden volgens de methode zoals beschreven in **B05 Incidentmanagement**.
* Levert input voor **B09 Veilig personeel**, waarin regels zijn opgenomen aangaande het uitgeven van toegangsrechten.
* Leidt tot de noodzaak van het uitvoeren van acties en het bijhouden van registraties. Deze staan weergegeven in de **jaarplanning informatiebeveiliging.**

*Normelementen*

* Annex 9.1.1: Beleid voor toegangsbeveiliging.
* Annex 9.1.2: Toegang tot netwerken en netwerkdiensten.
* Annex 9.2.1: Registratie en afmelden van gebruikers.
* Annex 9.2.2: Gebruikers toegang verlenen.
* Annex 9.2.3: Beheren van speciale toegangsrechten.
* Annex 9.2.4: Beheer van geheime authenticatieinformatie van gebruikers.
* Annex 9.2.5: Beoordeling van toegangsrechten van gebruikers.
* Annex 9.2.6: Toegangsrechten intrekken of aanpassen.
* Annex 9.3.1: Geheime authenticatieinformatie gebruiken.
* Annex 9.4.1: Beperking toegang tot informatie.
* Annex 9.4.2: Beveiligde inlogprocedures.
* Annex 9.4.3: Systeem voor wachtwoordbeheer.
* Annex 9.4.4: Speciale systeemhulpmiddelen gebruiken.
* Annex 9.4.5: Toegangsbeveiliging op programmabroncode.

# Voorwaarden

Voordat gestart kan worden met het inregelen van logisch toegangsbeheer moet voldaan zijn aan de volgende voorwaarden:

1. <organisatie> heeft een volledig overzicht van alle onderdelen van de infrastructuur waarvoor toegang verleend kan worden aan gebruikers. Onderdelen zijn: applicaties en netwerken.
2. <organisatie> heeft voor elk onderdeel een eigenaar aangewezen. Dat is degene die verantwoordelijk is voor adequaat onderhoud en beheer.
3. Van elk onderdeel bestaat een overzicht van de verschillende soorten rechten (rollen) die toegewezen kunnen worden aan gebruikers. Bijvoorbeeld in een applicatie wordt vaak onderscheiden: beheerder, gebruiker, teammanager etc.

# Toegangsbeheer

## Principes en regels

* Bij het verlenen van toegang tot informatie geldt het ‘need to know’ principe. Dat wil zeggen dat alleen toegang wordt verleend wanneer een medewerker dat nodig heeft voor het uitoefenen van zijn/haar functie. Er worden zo min mogelijk rechten verleend en deze rechten worden zo kort mogelijk verleend.
* Zo veel als mogelijk worden informatiesystemen van <organisatie> beveiligd middels 2-factor authenticatie. Dit is in overeenstemming met de resultaten van de afhankelijkheidsanalyse.
* Het is beheerders niet toegestaan om speciale systeemhulpmiddelen te gebruiken om in te loggen.
* Uitganspunt is dat alle toegangsrechten persoonlijk zijn. Dus per persoon geldt een unieke gebruikersnaam/wachtwoordcombinatie. Uitzonderingen hierop moeten bij voorkeur beperkt worden tot het minimaal haalbare, moeten worden goedgekeurd door de Directie en ze moeten worden geregistreerd.
* De eigenaar van draagt zorg voor periodiek controles op de autorisaties.

## Uitgifte wachtwoorden

Het is belangrijk dat initiële wachtwoorden op een veilige wijze worden overgedragen. Hiervoor gelden de volgende regels:

* Wanneer medewerkers toegang vragen tot een domein, wordt hun identiteit altijd geverifieerd door middel van fysieke verschijning, als dat niet mogelijk is, aan de hand van telefonisch navragen van identificerende gegevens.
* Wanneer medewerkers leveranciers toegang vragen tot een domein, wordt hun identiteit gecontroleerd door middel van navraag bij de contactpersoon van de organisatie waar zij werkzaam zijn.
* Een wachtwoord wordt nooit op de zelfde wijze als de inlognaam en/of URL van de toepassing gecommuniceerd.
* Een initieel wachtwoord moet aan de zelfde eisen voldoen als andere wachtwoorden.
* Initiële wachtwoorden moeten bij het eerste inlogmoment direct gewijzigd worden. Waar mogelijk moet dit technisch worden afgedwongen.
* Wanneer mogelijk moet de geldigheid van een initieel wachtwoord teruggebracht worden naar maximaal 2 dagen.

## Wachtwoordeisen

Binnen <organisatie> zijn sterke wachtwoorden verplicht. Eisen aan wachtwoorden moeten gecommuniceerd worden aan alle medewerkers, en waar mogelijk technisch worden afgedwongen. Er is een wachtwoordkluis beschikbaar gesteld aan medewerkers, waar wachtwoorden verplicht in opgeslagen moeten worden.

# Vaststellen doeltreffendheid

Jaarlijks beoordeelt de Security Officer of wordt voldaan aan onderstaande criteria. Dit bepaalt of dit beleidsdocument doeltreffend is.

## Criteria

De volgende criteria bepalen of de doeltreffendheid voldoende is:

* Maximaal 0 applicaties waarvan de rechten niet in de afgelopen 13 maanden zijn gecontroleerd.
* Maximaal 0 incidenten in de afgelopen 12 maanden omdat er voor onbevoegden toegang is geweest tot informatie, vanwege het verkeerd uitgegeven autorisaties.
* Maximaal 4 incidenten in de afgelopen 12 maanden omdat er voor onbevoegden toegang is geweest tot informatie, vanwege het niet voldoen aan het need-to-know principe.

In alle andere gevallen wordt de doeltreffendheid van dit document beoordeeld als onvoldoende.

## Controles en registraties

Voor het aantonen van bovenstaande criteria worden onderstaande controles minimaal jaarlijks uitgevoerd. De controles moeten op basis van de registraties reproduceerbaar zijn.

* Controleer of voor alle applicaties een autorisatierechtencontrole heeft plaatsgevonden in de afgelopen 13 maanden. Controleer voor applicaties met vertrouwelijkheidswaarde 5. Neem voor de overige applicaties een steekproef van 1 uit 2.
	+ Registratie: Uitvoerde en datum van de controle. Applicatie en eigenaar binnen de steekproef. Conclusie, met waar nodig vervolgstappen.
* Controleer of er in de afgelopen 12 maanden incidenten zijn gemeld, herleidbaar tot het verkeerd uitgeven van autorisaties en het niet voldoen aan het need-to-know principe.
	+ Registratie: Uitvoerder en datum van de controle. Aanpak analyse van incidenten. Conclusie, met waar nodig vervolgstappen.

*PS: Meld afwijkingen altijd als informatiebeveiligingsincident.*

## Administraties

Voor het uitvoeren van bovenstaande controles zijn de volgende administraties noodzakelijk:

* Controleverslagen autorisaties.