|  |
| --- |
| Richtlijn Autorisatiebeheer en -controle  Template |

|  |  |
| --- | --- |
| Auteur(s): |  |
| Versie: |  |
| Datum: | Kies of typ een datum |
| Kenmerk: |  |
|  |  |
|  |  |

**Documentinformatie**

Dit document maakt onderdeel uit van een complete set (beleidspiramide) met formeel vastgestelde documenten op strategisch, tactisch en operationeel niveau. Dit document heeft betrekking op de laag Richtlijn in de beleidspiramide.



**Versiebeheer**

|  |  |  |  |
| --- | --- | --- | --- |
| **Versie** | **Datum** | **Auteur** | **Verwerking** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Distributielijst**

|  |  |  |  |
| --- | --- | --- | --- |
| **Versie** | **Datum** | **Ontvanger** | **Doel** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Vaststelling**

|  |  |  |  |
| --- | --- | --- | --- |
| **Versie** | **Datum** | **Vastgesteld door** | **Vastgesteld op** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Samenhang met andere documenten**

|  |  |  |  |
| --- | --- | --- | --- |
| **Naam** | **Bovenliggend** | **Gelijk niveau** | **Onderliggend** |
| [INFORMATIEBEVEILIGINGSBELEID] | x |  |  |
| [STANDAARD IDENTITEIT EN TOEGANGSBEHEER | x |  |  |
| [DIVERSE RICHTLIJNEN |  | X |  |
|  |  |  |  |
|  |  |  |  |

**Verwijzingen naar SURFaudit Toetsingskader en ISO27001**

|  |  |
| --- | --- |
| **Kader** | **Verwijzing (tags)** |
| SURFaudit Toetsingskader | ID.01, SM.02, SM.11 |
| ISO27001 | A5, A8 |

**Creative Commons**

Afbeelding met symbool, schermopname, biljartbal

Automatisch gegenereerde beschrijvingDit template is een product van het SURF Security Expertise Centrum en beschikbaar onder de licentie Creative Commons Naamsvermelding 4.0 Internationaal. <https://creativecommons.org/licenses/by/4.0/deed.nl>

Inhoudsopgave

|  |
| --- |
| [Samenvatting 4](#_Toc196468612)  [1 Inleiding 5](#_Toc196468613)  [1.1 Doel 5](#_Toc196468614)  [1.2 Reikwijdte en Toepassingsgebied 5](#_Toc196468615)  [1.3 Rollen en Verantwoordelijkheden 5](#_Toc196468616)  [1.4 Definities en terminologie 6](#_Toc196468617)  [2 Richtlijn autorisatiebeheer en -controle 7](#_Toc196468618)  [2.1 Principes 7](#_Toc196468619)  [2.2 Toekennen van autorisaties 7](#_Toc196468620)  [2.3 Wijzigen en intrekken van autorisaties 7](#_Toc196468621)  [2.4 Periodieke controle van autorisaties 8](#_Toc196468622)  [2.5 Logging en Monitoring 8](#_Toc196468623)  [2.6 Continue verbetering 8](#_Toc196468624)  [3 Vaststelling 9](#_Toc196468625)  [Bijlage 1 Checklist Autorisatiecontrole 10](#_Toc196468626) |

Samenvatting

Hier komt een samenvatting, op zichzelf leesbaar, van de inhoud van dit document in max. 1 A4.

# Inleiding

Autorisatiebeheer en -controle vormen een onderdeel van het Identiteit- en Toegangsbeheer (IAM) binnen onze instelling. Effectief autorisatiebeheer zorgt ervoor dat gebruikers uitsluitend toegang hebben tot de informatie en systemen die nodig zijn voor de uitoefening van hun taken. Deze richtlijn beschrijft de vereisten en procedures die gehanteerd worden om toegang op een veilige en beheerste manier te waarborgen.

## Doel

Deze richtlijn heeft als doel een helder en eenduidig kader te bieden voor het beheren en controleren van autorisaties binnen onze instelling. Door het implementeren van duidelijke richtlijnen wordt de beschikbaarheid, integriteit en vertrouwelijkheid van informatie gewaarborgd.

## Reikwijdte en Toepassingsgebied

Het autorisatiebeheer en de controle hierop hebben betrekking op alle systemen en applicaties binnen onze instelling waarvoor toegangsbeheer noodzakelijk is. Dit geldt voor zowel interne medewerkers, studenten, onderzoekers als externe partijen, zoals leveranciers en partners, die toegang krijgen tot onze gegevens en IT-middelen.

## Rollen en Verantwoordelijkheden

Voor een effectief autorisatiebeheer moeten taken en verantwoordelijkheden duidelijk zijn toegewezen. Dit voorkomt misverstanden en draagt bij aan een efficiënte controle op toegangsrechten.

|  |  |
| --- | --- |
| **Rol** | **Verantwoordelijkheden** |
| Systeem- en applicatiebeheerders | Implementeren en beheren toegangsrechten en zorgen voor de naleving van de richtlijnen. |
| Leidinggevenden | Autoriseren en beoordelen toegangsrechten van hun teamleden. |
| Security Officers | Monitoren en controleren het autorisatiebeheer en rapporteren afwijkingen. |
| Auditteams | Autoriseren en beoordelen toegangsrechten van hun teamleden. |

## Definities en terminologie

|  |  |
| --- | --- |
| **Begrip** | **Toelichting** |
| Autorisatiebeheer | Het proces van toekennen, wijzigen en intrekken van toegangsrechten op basis van vastgestelde rollen en verantwoordelijkheden. |
| Autorisatiecontrole | De periodieke beoordeling van toegangsrechten om te waarborgen dat deze nog steeds in lijn zijn met de beveiligingsvereisten en functionele behoeften. |
| Least Privilege-principe | Het principe waarbij gebruikers alleen toegang krijgen tot de middelen die strikt noodzakelijk zijn voor hun functie. |
| Segregation of Duties (SoD) | Het scheiden van taken en verantwoordelijkheden om frauderisico's en belangenconflicten te minimaliseren. |

# Richtlijn autorisatiebeheer en -controle

Deze richtlijn beschrijft de principes, kaders en vereisten voor het effectief het toekennen, wijzigen en controleren van autorisaties (toegangsrechten).

## Principes

Bij het uitvoeren van autorisatiebeheer en -controles gaan we binnen onze instelling uit van de volgende principes.

* **Noodzakelijke toegang**

Toegangsrechten worden toegekend op basis van functionele noodzaak.

* **Least Privilege-principe**

Medewerkers krijgen alleen de rechten die zij nodig hebben voor hun werkzaamheden.

* **Periodieke controle**

Toegangsrechten worden minimaal jaarlijks beoordeeld en zo nodig aangepast.

* **Segregation of Duties (SoD)**

Kritieke taken worden gescheiden om ongeoorloofde activiteiten en fraude te voorkomen.

* **Traceerbaarheid en logging**

Alle wijzigingen in autorisaties worden geregistreerd en gecontroleerd.

* **Proportionaliteit en minimalisatie**

Toegangsrechten worden afgestemd op risico’s en minimale vereisten per functieprofiel.

## Toekennen van autorisaties

Het toekennen van autorisaties moet zorgvuldig en gecontroleerd gebeuren om risico’s op onbevoegde toegang te minimaliseren.

**Vereisten**

* De gebruiker of leidinggevende dient een aanvraag in via het toegangsbeheersysteem.
* De aanvraag wordt beoordeeld door een verantwoordelijke manager, als de aanvraag impact heeft of betrekking heeft op kritieke systemen of gegevens, wordt de data- dan wel de betreffende proceseigenaar betrokken.
* Na goedkeuring wordt de autorisatie geregistreerd en geïmplementeerd volgens de SOLL-matrix.
* Elke nieuwe autorisatie wordt gelogd en periodiek geëvalueerd.

## Wijzigen en intrekken van autorisaties

Het wijzigen en intrekken van autorisaties zorgt ervoor dat gebruikers niet langer toegang hebben tot systemen wanneer dat niet meer noodzakelijk is.

**Vereisten**

* Wijzigingen in autorisaties worden uitgevoerd op basis van functieaanpassingen of organisatorische wijzigingen.
* Bij vertrek of functiewijziging worden de niet langer benodigde rechten direct ingetrokken.
* Geautomatiseerde monitoring controleert op inactieve accounts en excessieve autorisaties (stapeling) van rechten.
* Logging en rapportage ondersteunen een effectieve controle en correctie van afwijkingen overeenkomstig onze Standaard Logging en Monitoring.

## Periodieke controle van autorisaties

Periodieke controle van autorisaties voorkomt dat ongewenste of te ruime autorisaties blijven bestaan.

**Vereisten**

* Minimaal jaarlijks worden toegekende autorisaties (IST) vergeleken met de SOLL-matrix.
* Afwijkingen worden geregistreerd en aangepast volgens het wijzigingsproces.
* Bevindingen uit de controle worden gerapporteerd aan het management.

## Logging en Monitoring

Logging en monitoring zorgen ervoor dat wijzigingen in autorisaties kunnen worden geanalyseerd en dat verdachte activiteiten tijdig worden opgemerkt.

**Vereisten**

* Alle wijzigingen in autorisaties worden vastgelegd en zijn raadpleegbaar voor auditdoeleinden.
* Monitoringtools detecteren ongebruikelijke toegangsactiviteiten en rapporteren deze.
* Actieve monitoring draagt bij aan het tijdig signaleren van risico’s en naleving van het beleid.

## Continue verbetering

Autorisatiebeheer moet voortdurend worden aangepast aan nieuwe dreigingen en technologische ontwikkelingen om een hoog beveiligingsniveau te garanderen.

**Vereisten**

* Evaluatieresultaten en auditbevindingen vormen de basis voor verbetermaatregelen.
* Verbeteringen worden periodiek doorgevoerd om risico’s te minimaliseren.
* Technologische ontwikkelingen en nieuwe dreigingen worden meegenomen in de doorontwikkeling van het autorisatiebeheer.

# Vaststelling

Deze richtlijn is aldus vastgesteld.

[Plaats], [Datum].

[NAAM]

[FUNCTIE].

[Na (her)vaststelling, ook de tabel op p.2 bijwerken]

1. Checklist Autorisatiecontrole

Deze checklist helpt bij het uitvoeren van een systematische controle op autorisaties binnen systemen en processen.

|  |  |  |  |
| --- | --- | --- | --- |
| **Systeem / proces in scope** |  | | |
| **Controle uitgevoerd door** | Naam | Functie | Datum |
| **Goedkeuring Business Owner** | Naam | Functie | Datum |

|  |  |  |  |
| --- | --- | --- | --- |
| **Controlepunt** | **Toelichting** | **Status** | **Actie vereist?** |
| Is er een actueel overzicht van alle gebruikers en hun autorisaties per systeem? | Overzicht moet regelmatig worden bijgewerkt en beschikbaar zijn voor audits. |  |  |
| Worden autorisaties periodiek gecontroleerd en bijgesteld? | Minimaal jaarlijks uitvoeren, inclusief verificatie door de business owner. |  |  |
| Worden nieuwe autorisaties goedgekeurd door de juiste verantwoordelijke? | Autorisatieaanvragen moeten worden goedgekeurd volgens het vastgestelde proces. |  |  |
| Worden autorisaties toegekend volgens het Least Privilege-principe? | Gebruikers krijgen alleen de minimale toegangsrechten die nodig zijn. |  |  |
| Zijn er procedures om autorisaties direct in te trekken bij uitdiensttreding of functiewijziging? | Directe intrekking voorkomt onnodige toegang en beveiligingsrisico’s. |  |  |
| Wordt Segregation of Duties (SoD) gewaarborgd? | Kritieke functies en verantwoordelijkheden moeten gescheiden zijn. |  |  |
| Is logging en monitoring ingeschakeld voor alle wijzigingen in autorisaties? | Toegangsrechten moeten volledig traceerbaar zijn. |  |  |
| Worden afwijkingen gerapporteerd en verwerkt conform het correctieproces? | Afwijkingen moeten worden geregistreerd en opgelost binnen een vastgesteld termijn. |  |  |
| Worden gebruikers regelmatig gewezen op hun verantwoordelijkheden t.a.v. autorisaties? | Training en bewustwording zijn essentieel voor een goed functionerend autorisatiebeheer. |  |  |
| Zijn er controles op inactieve accounts en ongebruikte rechten? | Accounts en rechten die niet langer nodig zijn moeten worden opgeschoond. |  |  |