|  |
| --- |
| Richtlijn Toekennen en Intrekken AutorisatiesTemplate |

|  |  |
| --- | --- |
| 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, ID.05 |
| ISO27001 | A5, A8 |

**Creative Commons**

Dit 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](#_Toc196469598)[1 Inleiding 5](#_Toc196469599)[1.1 Doel 5](#_Toc196469600)[1.2 Reikwijdte en Toepassingsgebied 5](#_Toc196469601)[1.3 Rollen en Verantwoordelijkheden 5](#_Toc196469602)[1.4 Definities 6](#_Toc196469603)[2 Richtlijn Toekennen en Intrekken van Autorisaties 7](#_Toc196469604)[2.1 Principes 7](#_Toc196469605)[2.2 Toekennen van Autorisaties 7](#_Toc196469606)[2.3 Intrekken van Autorisaties 8](#_Toc196469607)[2.4 Logging en Monitoring 8](#_Toc196469608)[2.5 Periodieke controle 8](#_Toc196469609)[2.6 Bewustwording en Training 8](#_Toc196469610)[2.7 Naleving en Handhaving 9](#_Toc196469611)[3 Vaststelling 10](#_Toc196469612) |

Samenvatting

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

# Inleiding

Het toekennen en intrekken van autorisaties 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 principes en vereisten voor de procedures die gehanteerd worden om toegang op een veilige en beheerste manier te waarborgen.

## Doel

Het doel van deze richtlijn is een helder en eenduidig kader te bieden voor het toekennen en intrekken van autorisaties binnen onze instelling. Door het implementeren van duidelijke richtlijnen worden de beschikbaarheid, integriteit en vertrouwelijkheid van informatie gewaarborgd.

## Reikwijdte en Toepassingsgebied

Deze richtlijn is van toepassing op alle systemen, applicaties en gegevensopslagen waarin autorisaties worden toegekend en beheerd. Dit geldt voor zowel interne medewerkers als externe gebruikers, inclusief geautomatiseerde accounts. De richtlijn bestrijkt initiële autorisatieverlening, wijzigingsverzoeken en het intrekken van rechten bij functiewijzigingen of uitdiensttreding.

## 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. |
| Functioneel beheerders | Coördineren de verwerking van autorisatieaanvragen en bewaken de naleving van de richtlijn. |
| Leidinggevenden | Autoriseren en beoordelen toegangsrechten van hun teamleden. |
| Security Officers | Monitoren en controleren het autorisatiebeheer en rapporteren afwijkingen. |
| Gebruikers | Dienen zich te houden aan de toegekende rechten en melden ongeautoriseerde toegang. |

## Definities

|  |  |
| --- | --- |
| **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 Toekennen en Intrekken van Autorisaties

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

## Principes

Bij het toekennen, wijzigen en intrekken van autorisaties gaan we binnen onze instelling uit van de volgende principes.

* **Toegekende autorisatie zijn eindig**

Toegangsrechten worden toegekend op basis van functionele noodzaak en zijn standaard voorzien van een einddatum.

* **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

Een formeel proces is vereist om ervoor te zorgen dat autorisaties op een veilige en controleerbare manier worden toegekend.

**Vereisten**

* Autorisatieaanvragen worden ingediend via een vastgesteld proces en bevatten de noodzakelijke motivatie.
* Alleen bevoegde personen (bijv. leidinggevenden, functioneel beheerders) kunnen een aanvraag indienen.
* Autorisaties worden goedgekeurd door een aangewezen verantwoordelijke op basis van de gevoeligheid van de toegangsrechten.
* Technische implementatie wordt uitgevoerd door systeembeheerders of geautomatiseerde processen.
* De aanvrager ontvangt een bevestiging en is verantwoordelijk voor de controle op correcte werking.

## Intrekken van Autorisaties

Het intrekken van autorisaties moet direct plaatsvinden zodra een medewerker, student of externe gebruiker geen toegang meer nodig heeft.

**Vereisten**

* Autorisaties worden onmiddellijk ingetrokken bij beëindiging van het dienstverband of contract.
* Functiewijzigingen en interne overplaatsingen vereisen een herbeoordeling van autorisaties.
* Accounts die 60 dagen niet zijn gebruikt, worden gedeactiveerd.
* Intrekkingen worden geregistreerd en geverifieerd door de verantwoordelijke afdeling.
* Gevoelige accounts worden gecontroleerd op restrechten na intrekking.

## Logging en Monitoring

Logging en monitoring zijn ingericht om wijzigingen in autorisaties te traceren en ongeautoriseerde toegang te detecteren.

**Vereisten**

* Alle wijzigingen in autorisaties worden gelogd met minimaal datum, gebruiker, type wijziging en goedkeurder.
* Periodieke controles worden uitgevoerd om naleving van procedures te bewaken.
* Afwijkingen in autorisatiebeheer worden onderzocht en waar nodig gecorrigeerd.

## Periodieke controle

Om te voorkomen dat onnodige of ongepaste rechten blijven bestaan, moeten autorisaties periodiek te worden gecontroleerd.

**Vereisten**

* Leidinggevenden zijn verantwoordelijk voor de periodieke beoordeling van autorisaties binnen hun afdeling.
* Toegewezen rechten worden geanalyseerd op actualiteit en noodzaak.
* Geconstateerde afwijkingen worden direct hersteld en gedocumenteerd.

Zie hiervoor onze ‘Richtlijn Autorisatiebeheer en -controle’.

## Bewustwording en Training

Een goed begrip van autorisatiebeheer bij medewerkers en leidinggevenden draagt bij aan een correcte naleving van deze richtlijn.

**Vereisten**

* Medewerkers worden periodiek geïnformeerd over hun rol en verantwoordelijkheden in autorisatiebeheer.
* Leidinggevenden en beheerders volgen gerichte training over processen en risico’s.
* Bewustwordingsprogramma’s worden ingezet om misbruik en nalatigheid in autorisatiebeheer te voorkomen.

## Naleving en Handhaving

Strikte naleving van deze richtlijn is noodzakelijk om beveiligingsrisico’s te beheersen.

**Vereisten**

* Niet-naleving kan leiden tot maatregelen volgens het interne sanctiebeleid.
* Periodieke controles en audits worden uitgevoerd om naleving te toetsen.
* Bevindingen uit audits worden vertaald in verbetermaatregelen.

# Vaststelling

Deze richtlijn is aldus vastgesteld.

[Plaats], [Datum].

[NAAM]

[FUNCTIE].

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