|  |
| --- |
| Standaard Identiteit- en ToegangsbeheerTemplate |

|  |  |
| --- | --- |
| 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 Standaard 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 |  |  |
| [LOGGING & MONITORING] |  | x |  |
| [LOGISCHE TOEGANG] |  |  | x |
| [FYSIEKE TOEGANG] |  |  | x |
| [MEERDERE PROCDURES] |  |  | x |

**Verwijzingen naar SURFaudit Toetsingskader en ISO Normen**

|  |  |
| --- | --- |
| **Kader** | **Verwijzing (tags)** |
| SURFaudit Toetsingskader | ID.01, ID.02, ID.03, ID.04, ID.05, SM.02 |
| ISO 27001:2022 | 5.7, 5.15, 5.16, 5.18, 5.19, 5.22, 5.28, 5.36 |
| ISO 24760 Part 2 | 2.2, 3.5, 3.7 |

**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](#_Toc187833664)[1 Inleiding 5](#_Toc187833665)[1.1 Doel 5](#_Toc187833666)[1.2 Toepassingsgebied en reikwijdte 5](#_Toc187833667)[2 Rollen, verantwoordelijkheden en bevoegdheden 6](#_Toc187833668)[3 Identiteitsbeheer 7](#_Toc187833669)[3.1 Doel 7](#_Toc187833670)[3.2 Principes 7](#_Toc187833671)[4 Toegangscontrole 8](#_Toc187833672)[4.1 Toewijzing van Toegangsrechten 8](#_Toc187833673)[4.2 Beheer van Bevoorrechte Toegang 8](#_Toc187833674)[4.3 Periodieke beoordeling van Toegangsrechten 8](#_Toc187833675)[4.4 Toegang van Externe Partijen 8](#_Toc187833676)[4.5 Beveiligingsvereisten voor Authenticatie 9](#_Toc187833677)[4.5.1 Single Sign-On (SSO) 9](#_Toc187833678)[4.6 Fysieke Toegangsbeveiliging 9](#_Toc187833679)[4.7 Monitoring en Logging van Toegang 9](#_Toc187833680)[4.8 Compliance en Audits 10](#_Toc187833681)[4.9 Gebruikersbewustzijn en Training 10](#_Toc187833682)[5 Rapportage en Borging 11](#_Toc187833683)[5.1 Rapportage 11](#_Toc187833684)[5.2 Borging 11](#_Toc187833685)[6 Vaststelling  12](#_Toc187833686)[Bijlage 1 Verklarende woordenlijst 13](#_Toc187833687) |

Samenvatting

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

# Inleiding

Dit document beschrijft de standaard identiteits- en toegangsbeheer, vanaf hier; IAM. De standaard definieert formele rollen, verantwoordelijkheden, principes en welke eisen worden gesteld aan het IAM proces. Het document volgt de indeling van ISO27001 en de richtlijnen uit ISO 24760 Part 2 (A framework for identity management – Reference architecture and requirements).

## Doel

Het doel van deze standaard is het beschermen van informatie en informatie verwerkende faciliteiten door effectieve toegangscontrole, beheer van identiteiten en autorisaties. Dit omvat zowel de fysieke toegang tot ruimten waar ICT-middelen zich bevinden als de toegang tot applicaties en ICT-componenten voor gebruikers en beheerders. Dit document beschrijft kaders en randvoorwaarden voor identiteitsbeheer. Werkwijzen voor logische en fysieke toegang worden in aparte (procedure)documenten beschreven.

## Toepassingsgebied en reikwijdte

Deze standaard is van toepassing op alle medewerkers, contractanten, bezoekers en andere personen die gerechtigd zijn tot toegang tot de faciliteiten of informatiesystemen van onze instelling, ongeacht de locatie van deze personen en/of systemen.

# Rollen, verantwoordelijkheden en bevoegdheden

Binnen het IAM proces zijn duidelijke rollen, verantwoordelijkheden en bevoegdheden belangrijk om effectief toepassen van toegangsrechten te waarborgen.

Binnen onze instelling onderscheiden we volgende rollen en verantwoordelijkheden:

|  |  |
| --- | --- |
|  Rol   | Verantwoordelijkheden   |
| **[Zelf invullen]** | * Ontwikkelt, onderhoudt en herziet het IAM-beleid.
* Verantwoordelijk voor communicatie van het beleid naar alle medewerkers.
 |
| **[Zelf invullen]** | * Toezicht op naleving van het IAM-beleid.
* Beheert risico’s met betrekking tot identiteiten en toegang.
* Voert risicoanalyses en aanpassingen door.
 |
| **Beheerder** | * Beheert de technische uitvoering van IAM, inclusief gebruikersbeheer.
* Beveiligt authenticatieprocessen en controleert logs.
* Meldt verdachte activiteiten.
 |
| **Teamleider** | * Keuren toegangsrechten goed voor medewerkers.
* Voeren periodieke toegangsreviews uit en informeren bij wijzigingen.
 |
| **Gebruikers** | * Naleven van het IAM-beleid en veilige wachtwoordpraktijken hanteren.
* Melden van incidenten en verantwoord gebruik van toegangsrechten.
 |
| **Auditors** | * Voeren audits uit om de naleving van het IAM-beleid te controleren.
* Rapporteren bevindingen en adviseren verbeteringen.
 |

# Identiteitsbeheer

## Doel

Het vaststellen van individuen en systemen (entiteiten) die toegang hebben tot informatie en andere relevante middelen van de instelling, zodat toegangsrechten aan een identiteit kunnen worden verleend en ingetrokken.

Een identiteit verwijst naar een unieke representatie van een persoon of systeem die toegang heeft tot informatie en bedrijfsmiddelen binnen de instelling. De identiteit omvat:

* **Identificatiegegevens**: Een unieke identificatie, zoals een gebruikersnaam of identificatienummer, die de entiteit onderscheidt van anderen.
* **Toegangsrechten**: Een set rechten en privileges die bepalen welke informatie en middelen toegankelijk zijn, inclusief lees-, schrijf- en wijzigingsrechten.
* **Verantwoordelijkheden**: De verplichting om verantwoordelijk te zijn voor handelingen die onder de identiteit worden uitgevoerd, met inachtneming van beveiligings- en gebruiksrichtlijnen.
* **Authenticatie-informatie**: Gegevens die nodig zijn voor verificatie, zoals wachtwoorden, tokens of biometrische gegevens.
* **Status**: Informatie over de huidige staat van de identiteit, zoals actief, inactief, gedeactiveerd of verwijderd, inclusief goedkeuringen voor gedeelde identiteiten of systeemtoegang.

## Principes

* **Toewijzing van Identiteiten**: Een identiteit wordt slechts aan één persoon toegewezen, zodat deze persoon verantwoordelijk kan worden gehouden voor alle handelingen die onder die identiteit plaatsvinden.
* **Gedeelde Identiteiten**: Gedeelde identiteiten (shared of group accounts) zijn alleen toegestaan indien operationeel noodzakelijk. Documentatie is vereist, onderbouwd met een risicoanalyse. Goedkeuring van het management is te allen tijde vereist.
* **Toewijzing aan Systemen**: Identiteiten toegewezen aan systemen worden gescheiden op basis van functionaliteit. Monitoring moet worden ingericht en goedkeuring van het management is te allen tijde vereist.
* **De-activatie van Identiteiten**: Identiteiten moeten tijdig worden gedeactiveerd of verwijderd zodra ze niet meer nodig zijn of niet meer gebruikt worden.
* **Unieke Koppeling**: Een identiteit kan slechts één keer aan een entiteit binnen een domein worden gekoppeld (geen dubbele identiteiten).
* **Registratie van Gebeurtenissen**: Alle belangrijke gebeurtenissen met betrekking tot het beheer van identiteiten en authenticatie moeten worden geregistreerd.

# Toegangscontrole

De regels voor het beheren van toegang tot systemen en informatie is gebaseerd op de principes “least privilege” en “need to know”. Toegang wordt verstrekt per identiteit, en nooit meer dan nodig voor de rol van de identiteit. De activiteiten voor toegang worden hieronder beschreven, uitgangspunt is dat deze activiteiten altijd gedocumenteerd worden.

## Toewijzing van Toegangsrechten

* **Role-Based Access Control (RBAC)**: Toegangsrechten worden toegewezen op basis van gebruikersrollen, waarbij rollen zijn gedefinieerd volgens de functie of verantwoordelijkheden van een gebruiker zoals vastgelegd in het bronsysteem.
	+ Voorbeeld: Een medewerker in de rol van 'Systeembeheerder' heeft andere toegangsrechten dan iemand in de rol van 'Financieel Medewerker'.
* **Attribute-Based Access Control (ABAC)**: Toegangsrechten worden toegekend op basis van attributen van de gebruiker, zoals locatie, tijdstip, of het type apparaat dat wordt gebruikt.
	+ Voorbeeld: Een gebruiker mag toegang krijgen tot bepaalde informatie alleen als hij zich binnen een bepaald netwerk bevindt en op bepaalde tijden inlogt.
* Toegangsrechten worden verleend op basis van een formeel autorisatieproces.
* Het proces van autorisatie wordt ondersteund door duidelijke documentatie en goedkeuring van de manager van de gebruiker.
* Aanpassingen in toegangsrechten worden vastgelegd in een wijzigingsbeheerproces.
* Beheerders moeten toezicht houden op wijzigingen in rechten en incidenten rapporteren.
* Rechten worden beperkt tot de minimale vereisten voor de rol. Dit geldt zowel voor logische als voor fysieke toegang.

## Beheer van Bevoorrechte Toegang

* Bevoorrechte identiteiten (zoals beheer accounts) worden strikt gecontroleerd en beperkt tot noodzakelijke gebruikers.
* Alle activiteiten van deze identiteiten worden gemonitord en gelogd.

## Periodieke beoordeling van Toegangsrechten

* Toegangsrechten worden regelmatig herzien om ervoor te zorgen dat ze nog steeds passend zijn voor de functie.
* Rechten worden aangepast en/of ingetrokken bij functiewijzigingen of het vertrek van medewerkers.

## Toegang van Externe Partijen

* Wanneer externe partijen, zoals leveranciers, toegang krijgen tot systemen, moeten strikte eisen worden gesteld, zoals tijdelijke toegangsrechten en monitoring. De eisen worden vastgelegd in het contract.
* Externe toegang moet regelmatig worden beoordeeld en indien nodig worden ingetrokken wanneer het contract of de samenwerking afloopt.

## Beveiligingsvereisten voor Authenticatie

Sterke wachtwoorden (zie procedure wachtwoorden) en multi-factor authenticatie (zie procedure MFA) worden gebruikt om de toegang te beveiligen. De methode voor MFA wordt per systeem bepaald en gedocumenteerd door de systeemeigenaar, gebaseerd op risicoanalyse.

Vereisten:

* Authenticatiegegevens worden beschermd en regelmatig gewijzigd volgens het beveiligingsbeleid.
* Voor wachtwoorden gelden de afspraken zoals vastgelegd in de procedure “wachtwoorden”.
* Authenticatiemiddelen moeten voldoen aan de beveiligingseisen beschreven in de IAM-richtlijnen.

### Single Sign-On (SSO)

Single Sign-On wordt toegepast om het gebruikersgemak te vergroten en de beveiliging van het authenticatieproces te verbeteren.

Vereisten:

* SSO mag alleen worden toegepast als het toegang biedt tot systemen die als niet-kritisch worden geclassificeerd, tenzij aanvullende maatregelen zijn getroffen (zoals monitoring en logging, risk based access control en periodieke controles op naleving en juist gebruik).
* SSO-implementaties moeten voldoen aan de beveiligingsvereisten voor authenticatie (MFA) en beschermd zijn tegen aanvallen zoals phishing en brute force.
* De toepassing van SSO moet worden gedocumenteerd en goedgekeurd door het management op basis van een risicoanalyse.

## Fysieke Toegangsbeveiliging

De beveiliging van fysieke toegang tot kritieke infrastructuur wordt beschreven in de procedure Fysieke Toegang. Deze procedure bevat richtlijnen voor:

* Toegangsmechanismen zoals sleutels, badges en biometrische verificatie.
* Autorisatieprocessen voor fysieke toegangsrechten.
* Het loggen en analyseren van fysieke toegangsactiviteiten.

## Monitoring en Logging van Toegang

* Alle toegangsactiviteiten, zowel fysiek als logisch, worden gelogd. Dit omvat datum, tijd, gebruikers-ID, locatie en bron van toegang.
* Logs van fysieke toegang bevatten onder andere informatie over de betreden ruimtes, gebruikte toegangsmechanismen (bijvoorbeeld badges of sleutels) en tijdstippen van toegang.
* Logs worden gegenereerd zoals beschreven in de standaard voor logging en monitoring.
* Logs worden bewaard zoals beschreven in de standaard voor logging en monitoring.
* Alle registraties bevatten minimaal de volgende gegevens: datum, tijdstip, locatie en identiteit van de gebruiker.
* Logs van fysieke en logische toegangsactiviteiten worden regelmatig beoordeeld om afwijkingen te detecteren en incidenten te voorkomen.
* Registratie- en trackingmechanismen moeten voldoen aan wettelijke eisen en organisatorisch beleid.

## Compliance en Audits

* Interne en Externe Audits: Toegangsrechten, processen en controles moeten regelmatig worden gecontroleerd door in- en externe auditors.
* Naleving van Wet- en Regelgeving: Toegangsbeheer moet voldoen aan relevante wet- en regelgeving, zoals de Algemene Verordening Gegevensbescherming (AVG).
* Bevindingen uit audits worden gerapporteerd aan het management, en corrigerende maatregelen worden vastgelegd en opgevolgd.
* Het auditprogramma houdt rekening met risico’s en kritieke systemen en wordt jaarlijks herzien.

## Gebruikersbewustzijn en Training

* Alle gebruikers ontvangen periodieke training over het belang van sterke wachtwoorden, multi-factor authenticatie (MFA) en veilig gebruik van toegangsrechten.
* Gebruikers worden getraind om bedreigingen zoals phishing-aanvallen te herkennen, die vaak gericht zijn op het verkrijgen van wachtwoorden of andere authenticatiegegevens.
* Specifieke rollen, zoals beheerders of auditors, krijgen aanvullende training die is afgestemd op hun verantwoordelijkheden binnen het IAM-proces.
* Het succes van trainingen wordt geëvalueerd door middel van awareness-tests of simulaties.

# Rapportage en Borging

Het doel van rapportage en borging is om inzicht te bieden in toegangsbeheer en ervoor te zorgen dat processen voldoen aan het beleid en wettelijke eisen.

## Rapportage

Rapportages worden elk kwartaal opgesteld en gepresenteerd aan het management en de CISO.

De rapportages omvatten:

* Aantal succesvolle en mislukte inlogpogingen.
* Toegangspogingen buiten werktijden.
* Activiteiten van bevoorrechte accounts.
* Resultaten van periodieke herzieningen van toegangsrechten en eventuele afwijkingen.

Incidenten met betrekking tot ongeautoriseerde toegang worden gedetailleerd beschreven in de rapportages.

## Borging

* De procesverantwoordelijke waarborgt dat IAM-processen consistent worden uitgevoerd.
* Regelmatige interne en externe audits controleren de naleving en effectiviteit van het toegangsbeheer.
* Structurele problemen of ernstige incidenten worden geëscaleerd naar het management of externe toezichthouders indien nodig.

# Vaststelling

Deze standaard is aldus vastgesteld.

[Plaats], [Datum].

[NAAM]

[HET COLLEGE / DE RAAD VAN BESTUUR].

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

1. Verklarende woordenlijst

|  |  |
| --- | --- |
| Onderdeel   | Beschrijving   |
| **ABAC (Attribute-Based Access Control)** | Een methode voor het beheren van toegang tot systemen en netwerken op basis van attributen van individuele gebruikers binnen een organisatie.    |
| **Audits** | Periodieke controles om de effectiviteit van fysieke en logische toegangsmaatregelen te evalueren en te zorgen dat deze voldoen aan de gestelde normen en regels.   |
| **Autorisatie en Beheer** | Het proces van toekennen, beheren en intrekken van toegangsrechten op basis van rollen, verantwoordelijkheden en behoefte tot toegang binnen de organisatie.   |
| **AVG (Algemene Verordening Gegevensbescherming):** | Europese privacywetgeving die de verwerking van persoonsgegevens reguleert.    |
| **CISO (Chief Information Security Officer)** | De leidinggevende verantwoordelijk voor de informatiebeveiliging binnen een organisatie.    |
| **Compliance en Auditing** | Waarborging dat toegangsbeveiligingsmaatregelen voldoen aan geldende wet- en regelgeving en interne beleidslijnen, inclusief het uitvoeren van audits.   |
| **Fysieke Toegangsbeveiliging** | Maatregelen voor fysieke toegang tot gebouwen, terreinen en specifieke beveiligde ruimtes.   |
| **IAM (Identity and Access Management)** | Een raamwerk van beleid, processen en technologieën voor het beheren van digitale identiteiten en toegangsrechten.    |
| **Identificatie en Authenticatie** | Processen om gebruikers te identificeren en hun identiteit te verifiëren (bijv. door wachtwoorden, biometrische gegevens of tokens) voordat toegang wordt verleend.   |
| **Logische Toegangsbeveiliging** | Maatregelen om de toegang tot digitale systemen, netwerken, applicaties en data te beheren en te beveiligen.   |
| **MFA (Multi-Factor Authenticatie)** | Een beveiligingsmechanisme waarbij gebruikers meerdere authenticatiemethoden moeten gebruiken om toegang te krijgen.    |
| **RBAC (Role-Based Access Control)** | Een methode voor het beheren van toegang tot systemen en netwerken op basis van de rollen van individuele gebruikers binnen een organisatie.    |
| **Regelgeving** | Het naleven van wet- en regelgeving, waarin eisen worden gesteld aan hoe toegang en gegevensbeveiliging moeten worden beheerd.   |
| **Registratie en Tracking** | Systemen voor het registreren en volgen van bezoekersbewegingen in gebouwen of specifieke ruimtes om te zorgen voor traceerbaarheid en naleving van beleid.   |
| **SSO (Single Sign-On)** | Een authenticatieproces dat gebruikers in staat stelt om met één set inloggegevens toegang te krijgen tot meerdere applicaties of systemen.    |
| **Toegangscontrole Systemen** | Systemen en processen voor het beheren van wie toegang heeft tot welke fysieke en digitale bronnen, inclusief identificatie, authenticatie en autorisatie.   |