|  |
| --- |
| Richtlijn Overlijden accounthouderTemplate |

|  |  |
| --- | --- |
| 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.02, ID.05 |
| ISO27001 | A5, A6, 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](#_Toc196476636)[1 Inleiding 5](#_Toc196476637)[1.1 Doel 5](#_Toc196476638)[1.2 Reikwijdte en Toepassingsgebied 5](#_Toc196476639)[1.3 Definities en terminologie 5](#_Toc196476640)[2 Richtlijn 6](#_Toc196476641)[2.1 Principes 6](#_Toc196476642)[2.2 Melden van overlijden 6](#_Toc196476643)[2.3 Blokkeren van accounts 6](#_Toc196476644)[2.4 Bewaring van gegevens 7](#_Toc196476645)[2.5 Toegang voor derden 7](#_Toc196476646)[2.6 Logging en controle 7](#_Toc196476647)[2.7 Communicatie en documentatie 7](#_Toc196476648)[3 Vaststelling 9](#_Toc196476649) |

Samenvatting

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

# Inleiding

Bij het overlijden van een accounthouder ontstaat een situatie waarin informatiebeveiliging, privacywetgeving en beheerprocedures samenkomen. Onze instelling dient zorgvuldig, transparant en rechtmatig om te gaan met accounts, toegangsrechten en (persoons)gegevens van overledenen. Deze richtlijn biedt kaders voor het beheer en de afhandeling van digitale toegangen en data van overleden gebruikers binnen de informatievoorziening van onze instelling.

## Doel

Deze richtlijn beschrijft principes en vereisten voor het omgaan met gebruikersaccounts en bijbehorende gegevens na het overlijden van een accounthouder. Hiermee wordt beoogd om risico’s op ongeautoriseerde toegang te beperken, gegevensbescherming te waarborgen en gelijktijdig de rechten van nabestaanden te respecteren binnen de kaders van wet- en regelgeving.

## Reikwijdte en Toepassingsgebied

Deze richtlijn is van toepassing op alle digitale accounts en identificerende middelen die onder beheer van onze instelling vallen, ongeacht het type accounthouder (intern, extern, tijdelijk). De richtlijn geldt voor alle functionarissen binnen onze instelling die betrokken zijn bij identiteit- en toegangsbeheer, gegevensverwerking of juridische toetsing van verzoeken met betrekking tot overledenen.

## Definities en terminologie

|  |  |
| --- | --- |
| **Term** | **Toelichting** |
| Accounthouder | Een natuurlijke persoon aan wie een gebruikersaccount is toegekend. |
| Nabestaanden | Familieleden of wettelijke vertegenwoordigers van de overledene. |
| Overlijdensmelding | Een officiële kennisgeving van overlijden, ondersteund met documentatie. |
| Erfrechtelijke vertegenwoordiging | Persoon die juridisch gemachtigd is namens de overledene op te treden. |
| Gegevensoverdracht | Overdracht van digitale informatie aan een gerechtigde derde partij. |

# Richtlijn

## Principes

De volgende principes liggen ten grondslag aan het handelen bij overlijden van een accounthouder.

* **Beveiliging voorop**

Accounts van overleden accounthouders worden beschouwd als potentiële risico-objecten en moeten tijdig worden afgeschermd.

* **Rechtmatigheid van toegang**

Gegevens mogen alleen worden ingezien of overgedragen aan personen met aantoonbare juridische bevoegdheid.

* **Privacybescherming blijft gelden**

Ook na overlijden is zorgvuldige omgang met persoonsgegevens verplicht.

* **Minimale gegevensverwerking**

Alleen strikt noodzakelijke gegevens worden verwerkt in het kader van deze richtlijn.

* **Transparantie richting nabestaanden**

Communicatie met betrokkenen geschiedt duidelijk en gecontroleerd.

## Melden van overlijden

Het zorgvuldig en controleerbaar vastleggen van een overlijdensmelding is belangrijk voor het in gang zetten van vervolgacties. De melding vormt het formele startpunt voor het blokkeren van toegang en het waarborgen van gegevensbescherming.

**Vereisten**

* Een overlijdensmelding moet worden ondersteund met een kopie van een officiële overlijdensakte.
* Bij verzoek tot gegevensoverdracht of inzage is ook een verklaring van erfrecht of andere juridische machtiging vereist.
* Meldingen en bijlagen worden geregistreerd als formele input voor beoordeling en verdere acties.

## Blokkeren van accounts

Om het risico op ongeautoriseerde toegang te minimaliseren, dient het gebruikersaccount na overlijden direct buiten gebruik te worden gesteld. Dit voorkomt onrechtmatige toegang tot systemen en (persoons)gegevens.

**Vereisten**

* Binnen één werkdag na verificatie van overlijden moet het gebruikersaccount worden geblokkeerd.
* Toegangsrechten, authenticatiemiddelen (zoals tokens, pasjes, certificaten) en rechten binnen systemen moeten worden ingetrokken.
* Het account wordt gemarkeerd als ‘inactief wegens overlijden’ in de centrale gebruikersadministratie.

## Bewaring van gegevens

Onze instelling moet voldoen aan bewaartermijnen en wettelijke verplichtingen met betrekking tot persoonsgegevens. Daarnaast moet er voldoende tijd zijn om rechtmatige verzoeken tot gegevensoverdracht te kunnen behandelen.

**Vereisten**

* Het gebruikersaccount en bijbehorende gegevens worden gedurende een bewaartermijn van zes maanden bewaard.
* Tijdens deze termijn kunnen gerechtigde partijen een verzoek tot gegevensoverdracht indienen.
* Na afloop van de bewaartermijn vindt verwijdering plaats volgens vastgestelde retentieprocedures, tenzij wet- of regelgeving anders vereist.

## Toegang voor derden

Inzage of overdracht van gegevens aan derden is alleen toegestaan wanneer zij aantoonbaar bevoegd zijn. De beoordeling hiervan vraagt om zorgvuldige toetsing en eenduidige besluitvorming.

**Vereisten**

* Alleen partijen met een geverifieerde erfrechtelijke of juridische bevoegdheid kunnen toegang of overdracht van gegevens verkrijgen.
* Verzoeken worden beoordeeld door een daartoe aangewezen functionaris met verantwoordelijkheid voor privacy, in afstemming met juridisch deskundige(n).
* Gegevensoverdracht geschiedt uitsluitend via beveiligde middelen en wordt geregistreerd.

## Logging en controle

Om de naleving van deze richtlijn te borgen en verantwoording mogelijk te maken, is een sluitende logging van alle handelingen vereist. Ook biedt dit inzicht in het tijdig en correct uitvoeren van acties.

**Vereisten**

* Alle handelingen met betrekking tot het account van een overleden accounthouder worden gelogd.
* Loggegevens worden minimaal 12 maanden bewaard voor auditdoeleinden tenzij hier andere verplichtingen gelden vanuit wet- of regelgeving.
* Er vindt periodiek controle plaats op de correcte toepassing van deze richtlijn.

## Communicatie en documentatie

Heldere en eenduidige communicatie met nabestaanden voorkomt misverstanden en draagt bij aan een respectvolle afhandeling. Ook documentatie over het verloop van de afhandeling is van belang voor transparantie en toetsbaarheid.

**Vereisten**

* Communicatie richting nabestaanden wordt uitgevoerd door daartoe bevoegde functionarissen.
* Informatie over rechten en procedures wordt duidelijk en neutraal verstrekt.
* Alle documentatie rondom de overlijdensmelding wordt centraal opgeslagen.

# Vaststelling

Deze richtlijn is aldus vastgesteld.

[Plaats], [Datum].

[NAAM]

[FUNCTIE].

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