|  |
| --- |
| Richtlijn Noodtoegang  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.04 |
| ISO27001 | 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](#_Toc196475984)  [1 Inleiding 5](#_Toc196475985)  [1.1 Doel 5](#_Toc196475986)  [1.2 Reikwijdte en Toepassingsgebied 5](#_Toc196475987)  [1.3 Definities en terminologie 5](#_Toc196475988)  [2 Richtlijn 6](#_Toc196475989)  [2.1 Principes 6](#_Toc196475990)  [2.2 Beheer van noodtoegang 6](#_Toc196475991)  [2.3 Verlening van noodtoegang 6](#_Toc196475992)  [2.4 Gebruik van noodtoegang 7](#_Toc196475993)  [2.5 Intrekken van noodtoegang 7](#_Toc196475994)  [2.6 Logging en evaluatie 7](#_Toc196475995)  [3 Vaststelling 8](#_Toc196475996) |

Samenvatting

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

# Inleiding

In uitzonderlijke situaties kan het noodzakelijk zijn om buiten de reguliere toegangsprocedures om toegang te verlenen tot informatiesystemen of gegevens. Deze vorm van toegang, aangeduid als noodtoegang, is belangrijk om de continuïteit van bedrijfsprocessen te waarborgen, incidenten te beheersen of schade te beperken. Tegelijkertijd brengt het verhoogde risico’s met zich mee die een zorgvuldige en gecontroleerde aanpak vereisen.

## Doel

Deze richtlijn beschrijft de principes en vereisten met betrekking tot het veilig verlenen, controleren en beëindigen van noodtoegang tot informatiesystemen. Noodtoegang is bedoeld om in uitzonderlijke situaties – waarin reguliere toegang niet mogelijk is – de continuïteit van kritieke processen of informatievoorziening te waarborgen, zonder afbreuk te doen aan beveiligings- en privacyprincipes.

## Reikwijdte en Toepassingsgebied

Deze richtlijn geldt voor alle informatiesystemen, accounts en gebruikers(groepen) binnen onze instelling waarvoor het verlenen van noodtoegang noodzakelijk of mogelijk is in geval van uitzonderlijke situaties. Hieronder vallen zowel interne als externe systemen, mits deze een rol spelen in het ondersteunen van kritieke bedrijfsprocessen binnen onze instelling.

## Definities en terminologie

|  |  |
| --- | --- |
| **Term** | **Toelichting** |
| Noodtoegang | Tijdelijke toegang tot systemen of gegevens buiten reguliere procedures, uitsluitend toegestaan in uitzonderlijke situaties waarin directe actie noodzakelijk is. |
| Break glass account | Een vooraf ingericht account met hoge rechten, uitsluitend te gebruiken in noodgevallen. |
| Noodsituatie | Een vooraf ingericht account met hoge rechten, uitsluitend te gebruiken in noodgevallen. |

# Richtlijn

Deze richtlijn bevat de principes en vereisten voor het verantwoord gebruik van noodtoegang binnen onze instelling. Daarbij wordt onderscheid gemaakt tussen het beheer, de verlening, het gebruik en de beëindiging van noodtoegang, evenals de noodzakelijke controles en bewustwordingsmaatregelen.

## Principes

Bij het verlenen en beheren van noodtoegang zijn de volgende principes binnen onze instelling leidend.

* Noodtoegang is uitsluitend toegestaan in aantoonbare noodsituaties.
* Het principe van minimale toegang (least privilege) blijft van kracht, ook bij noodtoegang.
* Elke vorm van noodtoegang is tijdelijk, aantoonbaar noodzakelijk en wordt zorgvuldig vastgelegd en geëvalueerd.
* Logging, monitoring en transparantie zijn verplicht voor alle activiteiten tijdens het gebruik van noodtoegang.
* Er wordt actief gestuurd op beperking van het gebruik van noodtoegang door alternatieve preventieve maatregelen.

## Beheer van noodtoegang

Het beheer van noodtoegang vereist specifieke beheersmaatregelen om het risico van misbruik of ongecontroleerde toegang te minimaliseren.

**Vereisten**

* Noodtoegang moet expliciet worden vastgelegd in het autorisatiebeheerproces.
* Break glass-accounts moeten centraal worden geregistreerd, voorzien zijn van sterke authenticatie en slechts toegankelijk zijn voor vooraf geautoriseerde functionarissen.
* Tijdelijke accounts voor noodtoegang moeten automatisch vervallen of handmatig worden ingetrokken na afloop van de noodsituatie.

## Verlening van noodtoegang

Voor het verlenen van noodtoegang gelden specifieke eisen ten aanzien van bevoegdheden, registratie en validatie.

**Vereisten**

* Alleen daartoe aangewezen functionarissen (zoals CISO, systeembeheerders of crisiscoördinatoren) mogen noodtoegang activeren.
* Elke activering van noodtoegang vereist een onderbouwde motivatie en zo mogelijk voorafgaande goedkeuring van de verantwoordelijke manager of CISO.
* De aanvraag en goedkeuring worden schriftelijk of digitaal vastgelegd, inclusief tijdstip en betrokken systemen.

## Gebruik van noodtoegang

Het gebruik van noodtoegang moet doelgericht en controleerbaar zijn.

**Vereisten**

* De toegang mag uitsluitend worden gebruikt voor het noodzakelijke doel zoals beschreven in de aanvraag.
* Elke handeling verricht onder een noodtoegang wordt volledig gelogd, inclusief gebruikersidentiteit, tijdstip en uitgevoerde acties.
* Indien mogelijk wordt het gebruik van noodtoegang real-time gemonitord door security operations.

## Intrekken van noodtoegang

Het tijdig intrekken van noodtoegang voorkomt langdurige blootstelling aan verhoogde risico’s.

**Vereisten**

* Toegang wordt direct ingetrokken zodra de noodsituatie is opgeheven.
* Direct bij intrekken worden het wachtwoord en andere kenmerken van het betreffende account gewijzigd.
* Bij automatische procedures wordt de toegang na een vooraf ingestelde periode ingetrokken.
* Een controle op achterblijvende toegangsrechten wordt standaard uitgevoerd.

## Logging en evaluatie

Noodtoegang vereist transparantie en controle achteraf.

**Vereisten**

* Na gebruik van noodtoegang wordt een evaluatie uitgevoerd door de verantwoordelijke security officer of functionaris.
* Loggegevens worden minimaal 12 maanden bewaard en zijn beschikbaar voor audits.
* Bevindingen uit evaluaties kunnen aanleiding geven tot verbetering van procedures en technische maatregelen.

# Vaststelling

Deze richtlijn is aldus vastgesteld.

[Plaats], [Datum].

[NAAM]

[FUNCTIE].

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