|  |
| --- |
| Template Fysieke beveiligingOndertitel |

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

**Documentinformatie**

Dit document maakt onderdeel uit van een complete set (piramide) met formeel vastgestelde documenten op strategisch, tactisch en operationeel niveau. Dit document heeft betrekking op de laag Thema-beleid 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 |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Verwijzingen naar SURFaudit Toetsingskader en ISO27001**

|  |  |
| --- | --- |
| **Kader** | **Verwijzing (tags)** |
| SURFaudit Toetsingskader | PH.01; PH.02 |
| ISO27001 | A.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](#_Toc156556860)[1 Inleiding 5](#_Toc156556861)[2 Algemene maatregelen 6](#_Toc156556862)[3 Fysieke toegang 7](#_Toc156556863)[Vaststelling 8](#_Toc156556864)[Bijlage: Maatregelen voor fysieke beveiliging 9](#_Toc156556865) |

Samenvatting

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

# Inleiding

Fysieke toegang tot netwerken, systemen en gegevens door onbevoegden levert een bedreiging op voor de vertrouwelijkheid, continue beschikbaarheid en integriteit van de informatie en informatieverwerking van [INSTELLING].

Met behulp van maatregelen voor fysieke beveiliging worden deze risico’s beperkt.

# Algemene maatregelen

[INSTELLING] heeft op basis van een specifiek op fysieke toegang tot netwerken, systemen en gegevens door onbevoegden gerichte risico-analyse bepaald welke maatregelen nodig zijn om deze toegang te verhinderen en tegelijkertijd de toegang van bevoegden, toegangsbewaking en de afhandeling van incidenten met toegangsverlening of -weigering, te faciliteren.

Deze risico-analyse en de maatregelen passen in het beleid van [INSTELLING] voor integrale veiligheid.

De goedgekeurde maatregelen zijn geïmplementeerd en omvatten ten minste:

* Maatregelen voor toegangsverlening voor betrokkenen bij [INSTELLING] en toegangsweigering (afsluiting) van onbevoegden tot de terreinen, gebouwen en interne zonering van [INSTELLING];
* Maatregelen voor de fysieke veiligheid van alle bij [INSTELLING] betrokkenen zodat compromittatie of hinder bij de uitvoering van hun werkzaamheden voor, namens of wegens [INSTELLING] wordt bestreden;
* Maatregelen voor de afscherming van gegevensdragers, bij verkrijging, opslag en gebruik, en afvoer van de gegevensdragers;

Hierbij zijn de eisen volgend uit beoogde of afgegeven certificering van de fysieke omgeving(en) van [INSTELLING] voor gebruiksgeschiktheid en beveiliging, onverkort geïmplementeerd.

In bijlage 1 is een overzicht opgenomen van de belangrijkste maatregelen.

[VERANTWOORDELIJKE VOOR FYSIEKE BEVEILIGING] is eigenaar en dus verantwoordelijk voor de juiste en doorlopende implementatie en toezicht op de fysieke toegang en bijbehorende maatregelen.

De doorlopende implementatie wordt door [VERANTWOORDELIJKE VOOR FYSIEKE BEVEILIGING] continu gecontroleerd.

Alle bij [INSTELLING] betrokkenen doen melding van gevonden gebreken in de fysieke beveiliging.

De risico-analyse(s) en maatregelimplementatie worden jaarlijks door de [VERANTWOORDELIJKE VOOR FYSIEKE BEVEILIGING] vernieuwd en tussentijds uitgevoerd voor ieder project dat wijziging beoogt van de fysieke infrastructuur van [INSTELLING].

# Fysieke toegang

[INSTELLING] hanteert in het bijzonder voor fysieke toegang de volgende regels:

[*Deze staan zo in het toetsingskader. Als je meer in detail wilt uitschrijven welke maatregelen hieronder vallen, neem ze dan op in de bijlage. Als een maatregel niet is geïmplementeerd of een alternatieve oplossing is gekozen, neem deze dan op in de uitzonderingenlijst zoals hieronder vermeld.*]

* De procedures voor registratie van (bezoekers)toegang zijn bekend en worden gehanteerd door alle [receptie- / facilitaire- / hospitality-] medewerkers;
* De toegang tot gebouwen, IT-ruimtes en rekencentra is met fysieke maatregelen beperkt;
* Toegang tot IT-ruimtes (MERs, SERs en andere fysieke zones, afdelingen of gebouwen) wordt alleen gegeven voor wie er toegang nodig heeft voor de taakuitvoering. Al deze toegang wordt gelogd en de logs worden beoordeeld door [verantwoordelijke voor fysieke toegang en/of de specifieke ruimte eigenaar];
* Alle medewerkers van [INSTELLING] dienen zichtbare identificatie te dragen. Bezoekers zijn geregistreerd en worden begeleid van toegang tot bestemming en terug;
* Jaarlijks herziet [verantwoordelijke voor fysieke toegang] in samenwerking met [Personeelszaken / HR] de fysieke-toegangsprofielen en laat aanpassingen binnen een [week] doorvoeren. [Personeelszaken / HR] informeert [verantwoordelijke voor fysieke toegang] over nieuwe en afzwaaiende medewerkers waarop [verantwoordelijke voor fysieke toegang] betreffende fysieke toegangsrechten aanpast.

Op basis van de risico-analyse zoals hierboven in paragraaf 2 genoemd, heeft [INSTELLING] besloten tot de volgende alternatieve maatregelen ten opzichte van hiervoor genoemde:

[Vul hier in wat je instelling niet doet, zoals ID-badges dragen – maar geef daarbij telkens aan wat de alternatieve oplossing is.]

# Vaststelling

Dit beleid is aldus vastgesteld.

[PLAATS], [DATUM].

[CISO / DIR IT / CIO].

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

1. Maatregelen voor fysieke beveiliging

[Geef hier een opsomming van de belangrijkste maatregelen en wie verantwoordelijk is voor implementatie/installatie en voor toezicht, plus verwijzingen naar procedures / procedurehand­boeken, logs, etc.]