|  |
| --- |
| Richtlijn Informatiebeveiliging binnen operationele ITIL-beheerprocessenTemplate |

|  |  |
| --- | --- |
| 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 KETENBEHEER] | x |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Verwijzingen naar SURFaudit Toetsingskader en ISO27001**

|  |  |
| --- | --- |
| **Kader** | **Verwijzing (tags)** |
| SURFaudit Toetsingskader | OP.03, CO.01, CO.02, IM.01, IM.02, IM.03, IM.04, CH.01, CH.02, CH.03, CH.04, CH.05, CH.06 |
| ISO27001 | 8.1, 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](#_Toc196470927)[1 Inleiding 5](#_Toc196470928)[1.1 Doel 5](#_Toc196470929)[1.2 Reikwijdte en Toepassingsgebied 5](#_Toc196470930)[1.3 Rollen en Verantwoordelijkheden 5](#_Toc196470931)[1.4 Definities 6](#_Toc196470932)[2 Richtlijn 7](#_Toc196470933)[2.1 Algemene principes 7](#_Toc196470934)[2.2 Incident Management 7](#_Toc196470935)[2.3 Change Management (Wijzigingen) 8](#_Toc196470936)[2.4 Problem Management 8](#_Toc196470937)[2.5 Configuration Management 9](#_Toc196470938)[2.6 Asset Management 9](#_Toc196470939)[2.7 Service Level Management 9](#_Toc196470940)[2.8 Access Management 10](#_Toc196470941)[2.9 Supplier Management 10](#_Toc196470942)[3 Vaststelling 11](#_Toc196470943) |

Samenvatting

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

# Inleiding

Deze richtlijn is een uitwerking van ons Strategisch Informatiebeveiligingsbeleid. Het beschrijft de principes en vereisten die voortvloeien uit informatiebeveiliging op de uitvoering van operationele ITIL-processen binnen onze instelling. De richtlijn is bedoeld voor iedereen die betrokken is bij IT-beheer en is van toepassing op interne en externe dienstverleners, inclusief ketenpartners. Deze richtlijn is beleidsbepalend en vormt de basis voor inrichting, uitvoering en toetsing van de processen. Procesbeschrijvingen zelf zijn in aparte documenten opgenomen.

## Doel

Het doel van deze richtlijn is het borgen van informatiebeveiliging binnen alle operationele ITIL-processen in onze instelling. Informatiebeveiliging beoogt het beschermen van de vertrouwelijkheid, integriteit en beschikbaarheid van informatie en systemen, en vormt een integraal onderdeel van ons servicemanagement.

Om dit te realiseren, sluiten we aan bij het principe van Continual Service Improvement (CSI) binnen ITIL, dat in de kern het Plan-Do-Check-Act (PDCA)-model volgt zoals toegepast binnen informatiebeveiliging. Hierdoor wordt de continue verbetering van beveiligingsmaatregelen en IT-diensten systematisch geborgd binnen de uitvoering van en samenwerking tussen operationele processen.

## Reikwijdte en Toepassingsgebied

Deze richtlijn is integraal onderdeel van het servicemanagement dat door en voor onze instelling wordt uitgevoerd en is van toepassing op de volgende ITIL-processen:

* Incident Management
* Change Management
* Problem Management
* Configuration Management
* Asset Management
* Service Level Management
* Access Management
* Supplier Management

## Rollen en Verantwoordelijkheden

|  |  |
| --- | --- |
| Rol | Verantwoordelijkheden |
| CISO | Vaststellen, evalueren en (laten) handhaven van deze richtlijn. Toezicht houden op naleving en uitvoering van maatregelen. |
| Proceseigenaar ITIL | Integreren van de vereisten uit deze richtlijn in het eigen procesgebied. Zorgen voor afstemming met informatiebeveiliging. |
| Servicemanager | Zorgen dat afgesproken beveiligingsmaatregelen worden opgenomen in SLA's en worden nageleefd. |
| Functioneel beheerder | Uitvoeren van maatregelen en signaleren van afwijkingen binnen het eigen applicatiegebied. |
| Technisch beheerder | Implementeren van technische maatregelen (zoals logging, back-up, toegangsbeheer) binnen infrastructuurcomponenten. |
| Security Officer | Adviseren over beveiligingsmaatregelen, uitvoeren van risicoanalyses, ondersteunen bij incident- en changemanagement. |
| Gebruiker | Naleven van beveiligingsmaatregelen, melden van incidenten en vertrouwelijk omgaan met informatie. |
| Leverancier | Leveren van diensten volgens overeengekomen beveiligingseisen en medewerking verlenen aan audits en monitoring. |

## Definities

|  |  |
| --- | --- |
| Begrip | Definitie |
| Asset | Elk item van waarde voor de organisatie, waaronder informatie, hardware, software en diensten. |
| CI (Configuration Item) | Elk onderdeel van de IT-infrastructuur dat beheerd wordt via Configuration Management en opgenomen is in de CMDB. |
| CMDB | Configuration Management Database – de centrale database waarin alle CIs en hun relaties worden beheerd. |
| CISO | Chief Information Security Officer – verantwoordelijk voor het informatiebeveiligingsbeleid en toezicht op uitvoering. |
| Change | Elke toevoeging, wijziging of verwijdering van iets dat invloed kan hebben op IT-diensten. |
| Incident | Elke gebeurtenis die niet tot de standaard werking van een dienst behoort en een onderbreking of vermindering van de dienst veroorzaakt. |
| MFA | Multi-Factor Authentication – authenticatiemethode waarbij meerdere verificatiestappen nodig zijn. |
| SLA | Service Level Agreement - Overeenkomst tussen aanbieder en afnemer waarin serviceniveaus en verantwoordelijkheden zijn vastgelegd. |
| Security Incident | Elk incident dat een (mogelijke) schending inhoudt van de vertrouwelijkheid, integriteit of beschikbaarheid van informatie. |

# Richtlijn

Dit hoofdstuk beschrijft de richtlijn in algemene principes en specifieke beveiligingseisen per operationeel ITIL-beheerproces. De eisen zijn aanvullend op het bestaande Service Management Beleid en vormen een kader voor de inrichting, uitvoering en borging van informatiebeveiliging in deze processen.

## Algemene principes

Aan de inrichting en uitvoering van de operationele ITIL-beheerprocessen liggen de volgende principes ten grondslag.

* **Risicogebaseerde aanpak**

Processen zijn zodanig ingericht dat risico's voor informatiebeveiliging worden geïdentificeerd, beoordeeld en beheerst.

* **Compliance**

Processen voldoen aantoonbaar aan interne beleidsregels, contractuele verplichtingen en relevante wet- en regelgeving (zoals de AVG, NIS2, WHO).

* **Security by Design**

Informatiebeveiliging wordt vanaf de initiële ontwerpfase structureel meegenomen in de inrichting van processen en systemen.

* **Eigenaarschap en verantwoordelijkheid**

Elke rol in een proces is gekoppeld aan verantwoordelijkheid voor de naleving van beveiligingseisen. Dit is geborgd in RACI-schema’s.

* **Transparantie en controleerbaarheid**

Inrichting en uitvoering van processen zijn aantoonbaar en controleerbaar.

* **Samenhang en integratie**

Informatiebeveiliging moet structureel geïntegreerd zijn in alle relevante ITIL-beheerprocessen. Beveiligingseisen worden verplicht meegenomen bij wijzigingen (change management), incidentafhandeling, configuratiebeheer en capaciteitsplanning.

## Incident Management

Incident Management is gericht op het zo snel mogelijk herstellen van verstoringen. Vanuit informatiebeveiliging gelden de volgende vereisten om tijdige detectie, correcte afhandeling en beheersing van beveiligingsincidenten te borgen.

**Vereisten**

* Incidenten met potentiële impact op vertrouwelijkheid, integriteit of beschikbaarheid van gegevens moeten expliciet als 'Security Incident' gemarkeerd worden.
* Prioriteitsstelling moet naast impact en urgentie ook security-criteria bevatten (bijv. datalek, integriteitsverlies, continuïteitsrisico).
* Beveiligingsincidenten (waaronder ook verdachte activiteiten) moeten binnen 1 uur worden gemeld aan het CISO-team.
* Alle incidenten worden vastgelegd in een uniforme centrale tool met logging, audit-trail en classificatie.
* Een 24/7-escalatiepad voor ernstige beveiligingsincidenten is verplicht.
* Informatie over beveiligingsincidenten mag uitsluitend beschikbaar zijn voor geautoriseerde functionarissen.
* Oorzaakanalyse van beveiligingsincidenten is verplicht binnen 5 werkdagen na afsluiting.
* Incidentafhandeling wordt geëvalueerd op verbeterpunten m.b.t. informatiebeveiliging.
* Processen bevatten een verplichte terugkoppeling naar bedrijfscontinuïteit- en back-upprocedures.
* Incident Management kent functiescheiding tussen registratie, opvolging en goedkeuring van afsluiting.

## Change Management (Wijzigingen)

Wijzigingen brengen risico's mee voor de stabiliteit en beveiliging van diensten, processen en systemen. Elk type change vereist passende beveiligingstoetsing en -maatregelen.

**Vereisten**

* Type wijzigingen (Standaard, Niet standaard, Spoed) kennen verschillende eisen m.b.t. informatiebeveiliging.
* Voor elke wijziging (Standaard, Niet standaard, Spoed) geldt een verplichte toetsing op informatiebeveiligingsimpact.
* Niet standaard en Spoed Changes vereisen expliciete risicobeoordeling en goedkeuring door ‘security’ (CISO-team of gemachtigde).
* Spoed Changes worden binnen 24 uur na uitvoering beoordeeld op impact op informatiebeveiliging.
* Changes die impact hebben op authenticatie, autorisatie, logging, encryptie of netwerksegmentatie mogen uitsluitend uitgevoerd worden met expliciete goedkeuring van ‘security’ (CISO-team of gemachtigde).
* In rollback- en testplannen moet staan hoe beveiliging hersteld wordt bij mislukking.
* Wijzigingen aan systemen met persoonsgegevens of vertrouwelijke bedrijfsdata moeten AVG-compliant zijn.
* Alle wijzigingen worden getoetst op functiescheiding, waarbij autorisatie, uitvoering en toetsing door verschillende rollen plaatsvindt.
* Wijzigingen met impact op continuïteit worden getoetst op hun effect op back-up, beschikbaarheid en herstelprocedures.

## Problem Management

Problem Management is gericht op het structureel oplossen van onderliggende oorzaken. Vanuit informatiebeveiliging is het van belang dat kwetsbaarheden structureel worden herkend en gemitigeerd.

**Vereisten**

* Root cause analyses van problemen moeten standaard een hoofdstuk “beveiliging” bevatten.
* Structurele kwetsbaarheden worden geregistreerd in het centrale ‘Risico Register’.
* Elke bevinding die duidt op een zwakke configuratie of onvoldoende logging, moet worden gedeeld met ‘security’ (CISO-team of gemachtigde).
* Lessons learned bij beveiligingsproblemen worden gedeeld met relevante ITIL-proceseigenaren.
* Problem Management sluit aan op Securityprocessen zoals Threat Intelligence en Vulnerability Management om beveiligingstrends vroegtijdig te onderkennen.
* Oplossingen die beveiliging raken (bijv. config-aanpassing, patching) vereisen validatie van effectiviteit door ‘security’ (CISO-team of gemachtigde).

## Configuration Management

Beveiligingsmaatregelen hangen sterk samen met actuele en correcte configuratiegegevens. De CMDB is hierin van belang en leidend.

**Vereisten**

* CI’s in de CMDB moeten worden voorzien van beveiligingsattributen: dataclassificatie, eigenaarschap, risicoprofiel.
* Configuraties van kritische assets (zoals firewalls, databases, IAM-systemen) moeten onder change control staan.
* Er moet een mechanisme zijn om ongeautoriseerde wijzigingen automatisch te detecteren.
* De integriteit van CI-data moet periodiek worden gevalideerd door middel van tooling en steekproeven.
* Alleen geautoriseerde functionarissen mogen wijzigingen aanbrengen in beveiligingsgevoelige CI’s.

## Asset Management

Beheer van assets moet borgen dat gegevensdragers en systemen beveiligd zijn gedurende de hele levenscyclus.

**Vereisten**

* Elk asset krijgt een beveiligingsclassificatie toegekend op basis van gevoeligheid en gegevenssoort.
* De eigenaar van een asset is verantwoordelijk voor de correcte beveiligingsmaatregelen.
* Afvoer of vervanging van assets vereist gecertificeerde datavernietiging of -wiping.
* Externe assets (cloud, mobiel, thuiswerk) moeten onder beveiligingsbeheer vallen, inclusief versleuteling en remote management.
* Gebruik van persoonlijke of externe devices is alleen toegestaan bij aantoonbare naleving van de beveiligingsstandaarden van onze instelling.
* Inventory moet volledig, actueel en geverifieerd zijn en onder toezicht staan.

## Service Level Management

Afspraken met interne en externe partijen over diensten en dienstverlening moeten expliciete beveiligingsparameters bevatten.

**Vereisten**

* SLA’s bevatten KPI’s en minimumeisen voor informatiebeveiliging (bijv. tijd tot respons op security-incidenten).
* Beveiligingsnormen (zoals ISO 27001) worden als referentie opgenomen in afspraken met leveranciers.
* Er is een periodieke SLA-review met expliciete security-evaluatie.
* Structurele overschrijdingen van beveiligingsnormen worden gemeld aan het CISO-team.

## Access Management

Ongeautoriseerde toegang vormt een van de grootste beveiligingsrisico’s. Toegangsbeheer moet strikt worden geregeld.

**Vereisten**

* Toegang tot systemen en gegevens gebeurt op basis van het need-to-know en least privilege principe.
* Rollen en rechten worden ten minste jaarlijks gereviewd door de verantwoordelijke informatie-eigenaar.
* Accounts van externe gebruikers (leveranciers, tijdelijk personeel) verlopen automatisch.
* Authenticatie dient MFA te ondersteunen bij kritieke systemen.
* Logging van toegang vindt centraal en geautomatiseerd plaats, en is technisch beschermd tegen wijziging achteraf.

## Supplier Management

Leveranciers spelen een sleutelrol in de keten. Zij moeten aantoonbaar voldoen aan beveiligingseisen.

**Vereisten**

* Contracten met leveranciers bevatten verplichte securityclausules, inclusief datalekmeldplicht en auditrechten.
* SLA’s bevatten minimaal eisen aan beschikbaarheid, herstel- en responstijden bij beveiligingsincidenten.
* Leveranciers moeten minimaal voldoen aan gelijkwaardige normen als de organisatie.
* Bij contractbeëindiging moeten toegang, data en configuraties gecontroleerd worden overgedragen en/of vernietigd.
* Periodieke evaluaties en (remote) audits op security-prestaties van de leverancier zijn verplicht.
* Inhuur van cloud- of SaaS-leveranciers vereist een toets vooraf op relevante security eisen en eisen vanuit wet- en regelgeving (zoals de AVG).

# Vaststelling

Deze richtlijn is aldus vastgesteld.

[Plaats], [Datum].

[NAAM]

[FUNCTIE].

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