|  |
| --- |
| Standaard KetenbeheerTemplate |

|  |  |
| --- | --- |
| 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 |  |  |
| [INKOOPBELEID] | x |  |  |
| [PROCEDURES ‘KETENBEHEER’] |  |  | x |
|  |  |  |  |

**Verwijzingen naar SURFaudit Toetsingskader en ISO27001, ISO27002 en ISO28000**

|  |  |
| --- | --- |
| **Kader** | **Verwijzing (tags)** |
| SURFaudit Toetsingskader | SC.01, SC.02, SC.03. SC.04 |
| ISO27001 | 4.4, 5.1, 5.2, 6.1, 6.2, 6.3, 6.4, 7.1, 7.2, 8.1, 8.2, 8.3, 8.4, 9.1, 9.2, 9.3, 10.1, 10.2, 10.3, 12.1, 12.2, 12.3, 12.4, 12.5, 12.6, 13.1, 14.1, 15.1, 16.1, 17.1, 18.1, 18.2 |
| ISO27002 | 5.1, 5.7, 5.12, 5.13, 5.18, 5.19, 5.23, 5.30, 5.34, 5.35, 5.36, 5.37, 5.38, 5.40, 8.1, 8.3, 8.4, 8.5, 8.7, 8.9, 8.10, 8.11, 8.16 |
| ISO28000 | 4.1, 4.2, 4.3, 4.4, 4.5, 5.2, 5.3, 5.4, 6.2, 6.3, 6.4, 8.2, 8.3, 8.4, 8.5, 9.1, 9.2, 9.3 |

**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](#_Toc192166194)[1 Inleiding 5](#_Toc192166195)[1.1 Doel 5](#_Toc192166196)[1.2 Reikwijdte en toepassingsgebied 5](#_Toc192166197)[1.3 Rollen en verantwoordelijkheden 5](#_Toc192166198)[2 Standaard Leveranciers- en Ketenbeheer 7](#_Toc192166199)[2.1 Principes 7](#_Toc192166200)[2.2 Selectie en Risicobeoordeling 7](#_Toc192166201)[2.3 Beveiligingseisen bij uitbestedingen 7](#_Toc192166202)[2.4 Contractbeheer 8](#_Toc192166203)[2.5 Evaluatie en Herziening van Contracten 8](#_Toc192166204)[2.6 Incidentbeheer en Continuïteit 9](#_Toc192166205)[2.7 Training en Bewustzijn voor Leveranciers 9](#_Toc192166206)[3 Monitoring en auditrechten 10](#_Toc192166207)[3.1 Monitoring van leveranciers en ketenpartners 10](#_Toc192166208)[3.2 Auditrechten en toetsing 10](#_Toc192166209)[4 Vaststelling 11](#_Toc192166210) |

Samenvatting

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

# Inleiding

Ketenbeheer is een belangrijk onderdeel van ons Strategisch Informatiebeveiligingsbeleid. Het helpt bij het beheersen van afhankelijkheden binnen samenwerkingsverbanden en draagt bij aan het verminderen van risico’s. Door ketens en leveranciers op een gestructureerde manier te beheren, wordt de betrouwbaarheid van processen vergroot en kan worden voldaan aan wettelijke en regelgevende eisen.

## Doel

Deze standaard beschrijft de principes, eisen en kaders voor ketenbeheer en leveranciersmanagement binnen onze instelling en is gebaseerd op internationaal erkende normen, zoals ISO 27001 en ISO 28000. Het doel is om een uniforme werkwijze te waarborgen voor het organiseren, controleren en beveiligen van ketenafhankelijkheden en leveranciersrelaties. Hiermee wordt bijgedragen aan de vertrouwelijkheid, integriteit en beschikbaarheid van onze informatie en systemen en de naleving van het Strategisch Informatiebeveiligingsbeleid van onze instelling.

## Reikwijdte en toepassingsgebied

Deze standaard is van toepassing op alle externe leveranciers, sub-leveranciers en partners die producten en/of diensten aan onze instelling leveren en daarbij gegevens van of voor ons verwerken. Deze partijen zijn verplicht om deze gegevens zorgvuldig en in overeenstemming met de door ons gestelde informatiebeveiligingseisen te beheren. Dit omvat onder meer leveranciers die verantwoordelijk zijn voor het verwerken, opslaan, overdragen of ondersteunen van gevoelige informatie.

De reikwijdte van deze standaard strekt zich uit tot het vaststellen van eisen voor het aangaan, beheren, monitoren en beëindigen van leveranciersrelaties. Daarnaast waarborgt de standaard dat informatiebeveiliging is geïntegreerd in alle fasen van de leveranciersketen, zodat onze gegevens en systemen te allen tijde beschermd zijn.

## Rollen en verantwoordelijkheden

Voor een effectieve uitvoering van deze standaard zijn rollen en verantwoordelijkheden vastgesteld. Het toewijzen van deze verantwoordelijkheden is van belang om te waarborgen dat informatiebeveiligingsrisico’s binnen de leveranciersketen op een consistente en gecontroleerde wijze worden beheerd.

* **CISO (Chief Information Security Officer)**
Verantwoordelijk voor het toezicht op de naleving van deze standaard en het beoordelen van leveranciersrisico’s. De CISO ziet erop toe dat alle beveiligingseisen correct worden geïmplementeerd en gehandhaafd.
* **Inkoopmanagement**
Verantwoordelijk voor het uitvoeren van risico-evaluaties bij de selectie van leveranciers en het waarborgen dat contractuele verplichtingen inzake informatiebeveiliging worden vastgelegd en nageleefd.
* **Contractmanagement**Verantwoordelijk voor het opstellen, beheren en bewaken van contractuele afspraken met leveranciers. Dit omvat het waarborgen van naleving van contractvoorwaarden, het monitoren van prestaties en het signaleren en mitigeren van contractuele risico’s. Daarnaast draagt contractmanagement bij aan het tijdig vernieuwen, herzien of beëindigen van contracten in lijn met de strategische doelstellingen van de organisatie.
* **Leveranciersmanagement**Richt zich op het beoordelen en continu monitoren van leveranciers om te garanderen dat zij voldoen aan de gestelde eisen op het gebied van kwaliteit, compliance en risicobeheersing. Dit omvat periodieke evaluaties van leveranciersprestaties, het onderhouden van relaties en het stimuleren van verbeteringen in samenwerking met leveranciers.
* **Afdeling IT**
Ondersteunt bij het technische beheer van leveranciers, inclusief het monitoren van de beveiliging van IT-infrastructuur die door leveranciers wordt gebruikt.
* **Gegevensverantwoordelijke**
Draagt de verantwoordelijkheid voor de gegevens die door leveranciers worden verwerkt en zorgt ervoor dat de verwerking voldoet aan interne en externe beveiligingseisen.

# Standaard Leveranciers- en Ketenbeheer

## Principes

Onze standaard voor Leveranciers- en Ketenbeheer is gebaseerd op de volgende principes die de basis vormen voor het beheer van informatiebeveiliging binnen de toeleveringsketen.

* **Risicogebaseerd beheer**
Beheersmaatregelen worden afgestemd op een gedegen risicobeoordeling waarbij beveiligingseisen in verhouding staan tot de potentiële impact van de leverancier.
* **Continuïteit en veerkracht**
Leveranciers moeten voorbereid zijn op verstoringen, met plannen voor bedrijfscontinuïteit en herstel die aantoonbaar regelmatig worden getest en beoordeeld.
* **Transparantie en verantwoording**
Leveranciers moeten inzicht geven in hun informatiebeveiligingsmaatregelen en voldoen aan rapportage- en auditverplichtingen om naleving en beveiliging te waarborgen.
* **Contractuele borging**
Beveiligingseisen worden vastgelegd in contracten, inclusief bepalingen over incidentbeheer, compliance en de plicht om te voldoen aan onze beveiligingsnormen.
* **Samenwerking en ketenbewustzijn**
Leveranciers werken actief met de instelling samen om beveiligingsrisico’s te beheersen en moeten zich bewust zijn van hun rol binnen de bredere toeleveringsketen, inclusief de beveiliging van subleveranciers.

## Selectie en Risicobeoordeling

Het selectieproces van leveranciers is ontworpen om naleving van beveiligingseisen en wet- en regelgeving, zoals AVG of de AI-Act, te waarborgen. Leveranciers worden beoordeeld op hun vermogen om gevoelige gegevens en systemen adequaat te beschermen, waarbij factoren zoals klantreferenties en relevante certificeringen, zoals ISO 27001, SOC 2 Type II, ISAE 3402 of vergelijkbare, worden geëvalueerd. Indien nodig worden on-site beoordelingen uitgevoerd om de fysieke en operationele beveiligingsmaatregelen te verifiëren.

Er worden maatregelen genomen om dreigingen binnen de toeleveringsketen te identificeren en aan te pakken. Dit is onderdeel van een risicobeoordeling volgens het risicomanagementbeleid.

Risico’s worden geclassificeerd op basis van de ‘classificatie van de applicatie’ en de toegangsniveaus van de leverancier en de impact op de instelling. Dreigingsinformatie wordt gebruikt om maatregelen te bepalen. Ook worden risico’s binnen de leveranciersketen geanalyseerd om dreigingen in de keten te onderkennen.

Dit proces is vastgelegd en wordt jaarlijks beoordeeld om de maatregelen actueel te houden.

## Beveiligingseisen bij uitbestedingen

Gegevens mogen alleen worden opgeslagen binnen vooraf overeengekomen regio’s, waarbij alle relevante wet- en regelgeving wordt nageleefd.

Leveranciers die verantwoordelijk zijn voor het uitvoeren van functies namens onze instelling, moeten passende beveiligingsmaatregelen implementeren. Dit omvat onder andere het waarborgen van de veiligheid van hun netwerkinfrastructuur en het beschermen van gegevens volgens minimaal de richtlijnen van onze instelling[[1]](#footnote-2).

Daarnaast moeten leveranciers ons informeren over beveiligingsupdates die van invloed kunnen zijn op onze systemen, zodat we de nodige maatregelen kunnen nemen.

De effectiviteit van de beveiligingsmaatregelen van leveranciers wordt regelmatig gecontroleerd door middel van geplande evaluaties en, indien nodig, aanvullende audits. Bij het constateren van afwijkingen of niet-naleving worden direct corrigerende maatregelen geëist, die vervolgens worden geëvalueerd om te garanderen dat de risico’s effectief worden beheerst.

Leveranciers moeten altijd kunnen aantonen dat hun maatregelen voldoen aan onze Strategisch Informatiebeveiligingsbeleid en onderliggende standaarden en richtlijnen.

## Contractbeheer

Het beheer van contracten met leveranciers is een integraal onderdeel van informatiebeveiliging. Contracten worden opgesteld in samenwerking met de afdeling Juridische Zaken en bevatten specifieke beveiligingsclausules die garanderen dat gevoelige informatie adequaat wordt beschermd. Deze clausules omvatten onder meer verplichtingen met betrekking tot:

* Incidentbeheer: Leveranciers dienen beveiligingsincidenten binnen een vastgestelde termijn te melden en passende maatregelen te nemen.
* Compliance: Leveranciers moeten aantonen dat zij voldoen aan relevante wet- en regelgeving en certificeringsnormen.
* Auditrechten: Onze instelling behoudt het recht om zowel geplande als ad-hoc audits uit te voeren ter controle op naleving van de afgesproken beveiligingseisen.
* Verantwoordelijkheid voor subleveranciers: Leveranciers zijn verplicht om onze beveiligingsvereisten contractueel door te voeren naar hun subleveranciers en hier aantoonbaar toezicht op te houden.
* Bij beëindiging van een contract moet de leverancier aantonen dat alle gegevens van de instelling zijn overgedragen en vervolgens verwijderd, of direct zijn verwijderd, en dat alle toegangsmogelijkheden zijn ingetrokken.
	+ Er moeten afspraken over geheimhouding van informatie ook na de beëindiging van de samenwerking nageleefd blijven.
	+ Een evaluatie van het beëindigingsproces wordt uitgevoerd om te controleren of alle verplichtingen zijn nagekomen. Dit omvat een verificatie van de genomen maatregelen en, indien nodig, aanvullende controles zoals audits of rapportages door de leverancier.

## Evaluatie en Herziening van Contracten

Contracten met leveranciers worden jaarlijks geëvalueerd om te controleren of ze nog voldoen aan de actuele beveiligings- en risicobeheervereisten, zoals vastgelegd in ons risicomanagementbeleid. Hierbij wordt rekening gehouden met veranderingen in de wet- en regelgeving, technologische ontwikkelingen en nieuwe beveiligingsdreigingen. Indien nodig worden de contractuele beveiligingseisen aangepast om te blijven voldoen aan onze instelling-eisen.

Het herzieningsproces is gedocumenteerd en wordt strikt nageleefd. Alle wijzigingen worden gevolgd en het management wordt op de hoogte gehouden van belangrijke updates en de bijbehorende risico’s.

## Incidentbeheer en Continuïteit

Het incidentbeheerproces is belangrijk om de impact van beveiligingsincidenten te minimaliseren en een snelle respons te garanderen. Leveranciers zijn verplicht een incidentmanagementproces te hanteren dat voorziet in:

* Een duidelijke definitie van beveiligingsincidenten en escalatieprocedures.
* Het onmiddellijk melden van incidenten die gevolgen kunnen hebben voor de informatiebeveiliging van onze instelling.
* Een gecoördineerde aanpak voor het analyseren, beheersen en oplossen van incidenten.
* Periodieke tests en evaluaties van incidentresponsprocedures om effectiviteit te waarborgen.
* Transparante communicatie over de aard en impact van incidenten, inclusief herstelmaatregelen.

Daarnaast dienen leveranciers ervoor te zorgen dat alle relevante medewerkers worden getraind in incidentdetectie en -respons. Evaluaties van incidentrapportages en opvolging van correctieve maatregelen maken aantoonbaar deel uit van het contractbeheerproces.

## Training en Bewustzijn voor Leveranciers

Leveranciers zijn verantwoordelijk voor het opleiden van hun medewerkers op het gebied van informatiebeveiliging. Alle medewerkers die betrokken zijn bij het verwerken of beheren van onze gegevens moeten een beveiligingstraining volgen die onderwerpen behandelt zoals toegangscontrole, databeveiliging, en incidentrespons. Deze trainingen dienen minimaal jaarlijks te worden herhaald om de kennis up-to-date te houden.

Bewustzijnsprogramma’s moeten ook worden geïmplementeerd om ervoor te zorgen dat medewerkers zich bewust zijn van beveiligingsrisico’s en de juiste procedures volgen. Leveranciers worden geacht bewijs van training en bewustmakingsactiviteiten te kunnen overleggen tijdens audits of evaluaties.

# Monitoring en auditrechten

Om de naleving van informatiebeveiligingseisen door leveranciers en ketenpartners te waarborgen, wordt een continu monitorings- en auditproces gehanteerd. Dit proces is afgestemd op de kaders uit het document Toetsing en Audit, waarin de organisatie van interne en externe toetsingen en audits is vastgelegd.

## Monitoring van leveranciers en ketenpartners

* Leveranciers worden continu gemonitord op naleving van contractuele beveiligingseisen en operationele prestaties.
* Afwijkingen en risico’s worden periodiek beoordeeld en geclassificeerd op basis van impact en waarschijnlijkheid.
* Voor leveranciers met een verhoogd risico worden aanvullende controles uitgevoerd, waaronder extra rapportageverplichtingen en intensievere audits.
* Er wordt gebruikgemaakt van zowel handmatige beoordelingen als geautomatiseerde monitoringtools om afwijkingen vroegtijdig te signaleren.

## Auditrechten en toetsing

* Onze instelling behoudt het recht om zowel geplande als ad-hoc audits uit te voeren bij leveranciers en subleveranciers.
* Leveranciers moeten aantonen dat hun beveiligingsmaatregelen voldoen aan de contractuele verplichtingen en vastgestelde normen.
* Periodieke audits worden uitgevoerd volgens de richtlijnen uit Toetsing en Audit, waarbij gebruik wordt gemaakt van interne controlemechanismen en onafhankelijke externe auditors.
* Leveranciers zijn verplicht om auditbevindingen te bespreken en correctieve maatregelen te implementeren binnen vastgestelde termijnen.
* De resultaten van audits en monitoring worden gerapporteerd aan de Chief Information Security Officer (CISO) en indien nodig aan andere relevante belanghebbenden.

# Vaststelling

Deze standaard is aldus vastgesteld.

[Plaats], [Datum].

[NAAM]

[FUNCTIE].

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

1. Zie ook bijlage B van SURF model VWO 4.0.: <https://pec.surf.nl/assets/surf-model-verwerkersovereenkomst-v4-0-nl/?category=processen> [↑](#footnote-ref-2)