|  |
| --- |
| Richtlijn Informatiebeveiliging binnen functioneelbeheer-processenTemplate |

|  |  |
| --- | --- |
| 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 |  |  |
| […] | x |  |  |
| [RICHTLIJN ITIL PROCESSEN] |  | 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](#_Toc202354085)[1 Inleiding 5](#_Toc202354086)[1.1 Doel 5](#_Toc202354087)[1.2 Reikwijdte en Toepassingsgebied 5](#_Toc202354088)[1.3 Rollen en Verantwoordelijkheden 5](#_Toc202354089)[1.4 Definities 6](#_Toc202354090)[2 Richtlijn 7](#_Toc202354091)[2.1 Algemene principes 7](#_Toc202354092)[2.2 Procescluster Gebruiksbeheer 7](#_Toc202354093)[2.3 Procescluster Functionaliteitenbeheer 8](#_Toc202354094)[2.4 Procescluster Verbindende processen – richtinggevend niveau 8](#_Toc202354095)[2.5 Procescluster Verbindende processen – uitvoerend niveau 8](#_Toc202354096)[2.6 Procescluster Sturende processen 9](#_Toc202354097)[2.7 Procescluster Opstellen Informatiestrategie 9](#_Toc202354098)[2.8 Procescluster IV-organisatiestrategie 9](#_Toc202354099)[3 Vaststelling 10](#_Toc202354100) |

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. Zij beschrijft de principes en vereisten die voortvloeien uit informatiebeveiliging op de uitvoering van operationele processen van functioneel beheer. Voor de uitwerking is het Business Information Services Library (BiSL)-framework als leidraad genomen. BiSL biedt een gestructureerde en algemeen erkende procesindeling die breed wordt toegepast binnen het onderwijs en onderzoek, en sluit goed aan op de praktijk van functioneel beheerders en informatiemanagers.

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 om informatiebeveiliging structureel te borgen binnen alle operationele BiSL-processen van onze instelling. De richtlijn vertaalt de strategische uitgangspunten uit het Strategisch Informatiebeveiligingsbeleid naar concrete eisen op procesniveau binnen het functioneel beheer, zoals beschreven in het BiSL-framework.

## Reikwijdte en Toepassingsgebied

Deze richtlijn is integraal onderdeel van het functioneel beheer dat door en voor onze instelling wordt uitgevoerd en is van toepassing op alle BiSL-processen in de clusters:

* Gebruiksbeheer
* Functionaliteitenbeheer
* Verbindende processen – richtinggevend niveau
* Verbindende processen – uitvoerend niveau
* Studerende processen
* Opstellen informatiestrategie
* IV-organisatiestrategie

## Rollen en Verantwoordelijkheden

|  |  |
| --- | --- |
| Rol | Verantwoordelijkheden |
| CISO | Vaststellen, evalueren en handhaven van deze richtlijn. Bewaken van de aansluiting op het strategisch informatiebeveiligingsbeleid. Toezicht op uitvoering en naleving. |
| Proceseigenaar BiSL | Integreren van de beveiligingsvereisten uit deze richtlijn in de betreffende BiSL-processen. Toezien op naleving binnen het domein. |
| Servicemanager | Zorgen dat afgesproken beveiligingsmaatregelen worden opgenomen in SLA's en worden nageleefd. |
| Functioneel beheerder | Uitvoeren van beveiligingsmaatregelen in de praktijk. Signaleren van afwijkingen. Input leveren voor impactanalyses en wijzigingen. |
| Technisch beheerder | Implementeren van technische beveiligingsmaatregelen (zoals logging, toegangsbeheer, versleuteling). Afstemmen met functioneel beheer. |
| Security Officer | Adviseren over beveiliging, uitvoeren van risicoanalyses, begeleiden van incidentafhandeling en risicobeheersing. |
| Gebruiker | Naleven van beveiligingsmaatregelen. Bewust omgaan met informatie. Melden van incidenten of onregelmatigheden. |
| Leverancier | Leveren van diensten conform overeengekomen beveiligingseisen. Samenwerken bij monitoring, evaluaties en audits. |

## Definities

|  |  |
| --- | --- |
| Begrip | Definitie |
| Risicoanalyse | Analyse waarbij de impact van een wijziging of gebeurtenis op de beschikbaarheid, integriteit en vertrouwelijkheid van informatievoorziening wordt vastgesteld. |
| Functioneel beheer | Activiteiten die zorgen dat de informatievoorziening aansluit bij de behoeften van gebruikers en processen, inclusief wijzigingsverzoeken en acceptatie. |

# Richtlijn

Dit hoofdstuk beschrijft de richtlijn in algemene principes en specifieke beveiligingseisen per BiSL-procescluster. De eisen zijn aanvullend op de Richtlijn Informatiebeveiliging in operationele ITIL-processen en vormen een kader voor de inrichting, uitvoering en borging van informatiebeveiliging binnen deze processen.

## Algemene principes

Aan de inrichting en uitvoering van de BiSL-processen 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 en Privacy by Design**

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

* **Security en Privacy by Default**

Diensten en systemen die binnen de BiSL-processen worden beheerd, worden standaard veilig en privacy vriendelijk ingericht.

* **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 BiSL-processen. Beveiligingseisen worden verplicht meegenomen bij het opstellen van specificaties, wijzigingsvoorstellen, gebruikersinstructies, en evaluaties van het gebruik van informatiesystemen.

## Procescluster Gebruiksbeheer

De processen binnen dit procescluster zijn gericht op het ondersteunen van gebruikers bij het dagelijks gebruik van de informatievoorziening, het beheren van gegevens en rechten, en het afstemmen met de operationele keten. Vanuit informatiebeveiliging gelden de volgende vereisten om de beschikbaarheid, integriteit en vertrouwelijkheid van informatie tijdens dagelijks gebruik en interactie met gebruikers te borgen.

**Vereisten**

* Beveiligingsincidenten moeten via het meldproces snel en correct worden geëscaleerd.
* Logging en monitoring van gebruikersactiviteiten zijn ingericht met inachtneming van de AVG, met duidelijke doelen zoals incidentdetectie en misbruikpreventie. Gebruikers worden hierover vooraf geïnformeerd.
* Gebruikers ontvangen instructies over veilig gebruik, phishing, wachtwoordbeheer, en het melden van incidenten.
* Gebruikersrechten worden strikt toegekend volgens onze ‘Standaard Identiteit- en Toegangsbeheer’.
* Proces voor periodieke controle op autorisaties is ingericht.
* Bij overdracht van gegevens tussen ketenpartners is transport beveiligd volgens onze ‘Standaard Cryptografie.

## Procescluster Functionaliteitenbeheer

De processen binnen dit procescluster zijn gericht op het specificeren, realiseren en toetsen van wijzigingen in de informatievoorziening, zowel geautomatiseerd als niet-geautomatiseerd. Vanuit informatiebeveiliging gelden de volgende vereisten om risico’s bij veranderingen in systemen en processen te beheersen en veilige implementatie van wijzigingen te borgen.

**Vereisten**

* Informatiebeveiliging is een integraal onderdeel van requirements en functionele specificaties.
* Risicoanalyses worden uitgevoerd voor alle voorgestelde wijzigingen.
* Testplannen bevatten expliciet beveiligingstesten (bijv. penetratietests, autorisatietests).
* Wijzigingen worden alleen doorgevoerd na expliciete goedkeuring.
* Back-outplannen (rollback) zijn verplicht voor wijzigingen met potentieel beveiligingsrisico.

## Procescluster Verbindende processen – richtinggevend niveau

De processen binnen dit procescluster zijn gericht op de afstemming tussen informatiestrategie en IV-organisatiestrategie, met als kernproces Informatiecoördinatie. Vanuit informatiebeveiliging gelden de volgende vereisten om structurele borging van beveiligingsdoelstellingen in strategische besluitvorming te realiseren.

**Vereisten**

* Informatiebeveiliging is expliciet opgenomen als toetsingscriterium bij afstemming van informatiestrategieën.
* Beveiligingsaspecten worden structureel afgestemd met andere domeinen zoals architectuur, compliance, data governance.
* Interne en externe afhankelijkheden worden in kaart gebracht en beveiligingsmaatregelen worden afgestemd.

## Procescluster Verbindende processen – uitvoerend niveau

De processen binnen dit procescluster zijn gericht op het coördineren en begeleiden van transities en wijzigingen binnen de informatievoorziening, zoals Wijzigingenbeheer en Transitie. Vanuit informatiebeveiliging gelden de volgende vereisten om beveiligingsrisico’s tijdens veranderingen beheersbaar te houden en integriteit van de informatievoorziening te waarborgen.

**Vereisten**

* Voor elke wijziging wordt een risicoanalyse (wat is de impact op beschikbaarheid, integriteit en vertrouwelijkheid) uitgevoerd.
* Wijzigingen worden ingedeeld naar risicoprofiel (laag, midden, hoog) met passende beheersmaatregelen.
* Acceptatiecriteria bevatten expliciete beveiligingseisen.
* Transitieplannen bevatten controlepunten voor beveiligingsrisico’s.

## Procescluster Sturende processen

De processen binnen dit procescluster zijn gericht op het stellen van tactische kaders aan de uitvoering van de informatievoorziening, zoals behoeftemanagement, kwaliteitsmanagement en financieel management. Vanuit informatiebeveiliging gelden de volgende vereisten om beheersing van risico’s en sturing op beveiligingseisen op tactisch niveau te garanderen.

**Vereisten**

* Kwaliteitsmanagement bevat criteria voor informatiebeveiliging (bijv. ISO 27001-conformiteit).
* Budgetten voor functioneel beheer bevatten gereserveerde middelen voor beveiligingsmaatregelen.
* Behoeftemanagement zorgt voor structurele vertaling van beveiligingsbehoeften naar eisen.
* KPI’s voor volwassen informatiebeveiliging zijn onderdeel van sturingsinformatie (bijv. incidenten, bevindingen uit audits).

## Procescluster Opstellen Informatiestrategie

De processen binnen dit procescluster zijn gericht op het formuleren van lange termijnvisie en -beleid voor informatievoorziening. Vanuit informatiebeveiliging gelden de volgende vereisten om strategische borging van beveiliging in toekomstige ontwikkelingen te verzekeren.

**Vereisten**

* Informatiebeveiliging is een strategisch uitgangspunt in lifecyclemanagement en portfoliomanagement.
* Technologische ontwikkelingen worden beoordeeld op implicaties voor informatiebeveiliging (bijv. cloud, AI, quantum).
* Beveiligingseisen worden vastgelegd in architectuurprincipes.

## Procescluster IV-organisatiestrategie

De processen binnen dit procescluster zijn gericht op de inrichting en governance van de IV-organisatie, inclusief ketenpartners en leveranciers. Vanuit informatiebeveiliging gelden de volgende vereisten om verantwoordelijkheden, afspraken en toezicht op beveiliging binnen de gehele IV-keten te borgen.

**Vereisten**

* Beveiligingseisen worden opgenomen in leverancierscontracten en SLA’s.
* Er zijn processen ingericht voor toezicht op de beveiligingsmaatregelen van ketenpartners.
* Relatiemanagement bevat afspraken over gezamenlijke beveiligingsdoelstellingen.
* Evaluatie van leveranciersprestaties bevat beveiligingscriteria.

# Vaststelling

Deze richtlijn is aldus vastgesteld.

[Plaats], [Datum].

[NAAM]

[FUNCTIE].

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