|  |
| --- |
| Template Risico Acceptatie Overeenkomst‘Naam’ risico |

|  |  |
| --- | --- |
| 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 Procedure 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 |  |  |
| [BELEID RISICOBEHEER] | x |  |  |
| [PROCEDURE RISICOBEHEER] | x |  |  |
|  |  |  |  |
|  |  |  |  |

**Verwijzingen naar SURFaudit Toetsingskader**

|  |  |
| --- | --- |
| **Kader** | **Verwijzing (tags)** |
| SURFaudit Toetsingskader | RM.01, RM.02, RM.03 |
|  |  |

**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](#_Toc192754339)[1 Inleiding 5](#_Toc192754340)[2 Beschrijving risico 6](#_Toc192754341)[3 Voorgestelde maatregelen 7](#_Toc192754342)[4 Genomen besluit 8](#_Toc192754343) |

Samenvatting

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

|  |
| --- |
| SAMENVATTING |
| Referentienummer | RA.23-01 (voorbeeld) |
| Datum | DD MM YYYY |
| Systemen en/of processen | Betrokken systemen en processen |
| Korte beschrijving risico | Wat houdt het risico in? |
| Risico inschatting | Laag/Gemiddeld/Hoog/Zeer Hoog |
| SURF Control(s) | SURFaudit Toetsingskader Infomatiebeveiliging referenties |
| Eigenaar (‘accountable’) | Naam en Functie |
| Actiehouder (‘responsible’) | Naam en Functie |
| Actie | Acceptatie |
| Vervaldatum | DD MM YYYY |

# Inleiding

Het huidige beleid vereist het treffen van passende maatregelen ter bescherming van informatie en van <het/de systeem/omgeving/werkwijze/proces> dat onder verantwoordelijkheid valt van <naam eigenaar/verantwoordelijke >.

Binnen <dit/deze systeem/omgeving/werkwijze/proces> is er een risico aanwezig als gevolg van <risicobeschrijving>.

Dit risico is in het volgende hofdstuk 2 verder uitgeschreven en vanuit risicobeheer wordt een advies gegeven hoe met het onderkende risico moet worden omgegaan.

Deze Risico Acceptatie Overeenkomst (RAO) is geldig tot de volgende frequenties per risiconiveau:

* Zeer Hoog: maximaal 3 maanden
* Hoog: maximaal 6 maanden
* Gemiddeld: maximaal 1 jaar

De RAO wordt in het risicoregister opgenomen en moet geëvalueerd worden na het verstrijken van de verlooptijd. In het geval van een significante wijziging in de risico's zal deze evaluatie eerder plaatsvinden.

# Beschrijving risico

[Beschrijf hier het risico inclusief de bestaande maatregelen]

Het risico wordt ingeschat als**:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Kans |  | Impact |  | Risico |
| [kans niveau] | X | [impact niveau] | = | risiconiveau |

Pas de tabel hieronder om het ingeschatte risico weer te geven (gebruik het template Risico-matrix voor de juiste termen en kleuren.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **RISICO SCORE**(kans \* impact) | **Kans 1**Zeer klein | **Kans 2**Klein | **Kans 3**Gemiddeld | **Kans 4**Groot | **Kans 5**Zeer Groot |
| **Impact 1**Verwaarloosbare  |  |  |  |  |  |
| **Impact 2**Klein |  |  | **Gemiddeld** |  |  |
| **Impact 3**Gemiddeld |  |  |  |  |  |
| **Impact 4**Grote |  |  |  |  |  |

# Voorgestelde maatregelen

[Beschrijf welke maatregelen er genomen kunnen worden, wat de kans en impact zijn na het nemen van de maatregelen en wat het resterende risiconiveau is na het nemen van de maatregelen]

# Genomen besluit

[Beschrijf hier de volgende zaken:

* Indien van toepassing (afhankelijk van de vastgestelde risicobereidheied): welke maatregelen genomen worden om het risico acceptabel te maken
* Motivatie bij acceptatie van het risico
* Geldigheid acceptatie / datum volgende evaluatie in lijn met de frequenties per risiconiveau]

|  |  |
| --- | --- |
| Risiconiveau | Benodigde beoordelingen en/of goedkeuringen |
| Laag | **N.v.t. – impliciete acceptatie.** |
| Gemiddeld | **Risicoacceptatie:** Risico-eigenaar kan het risico accepteren, mits de risicobereidheid niet wordt overschreden. Consultatie van ISO/BSO is aanbevolen. |
| Hoog | **Risicoacceptatie:** Risico-eigenaar kan het risico accepteren na consultatie van ISO/BSO (verplicht), mits de risicobereidheid niet wordt overschreden. ISO/BSO kan de CISO consulteren (optioneel). |
| Zeer hoog (**niet** faculteit/divisie overstijgend)  | **Risicoacceptatie:** Consultatie bij CISO is verplicht waarna het faculteitsbestuur (of equivalent gremium) het risico kan accepteren. |
| Zeer hoog (faculteit/divisie overstijgend) | **Risicoacceptatie:** Consultatie bij CISO is verplicht waarna alleen acceptatie mogelijk is door het CvB. |

[In plaats van ‘natte’ handtekeningen volstaat een email vanaf het instellings emailaccount van de betrokken functionaris aan ‘ciso@........nl’ of een van de ISO/BSOs/…… onder vermeldingen van het registratienummer RA.xx.xx. Voeg als bewijs een kopie van de email toe in het handtekening vak]

**Goedkeuringen:** *<te gebruiken bij gemiddeld risico,**verwijder indien niet van toepassing>*

|  |  |
| --- | --- |
| Systeemeigenaar/proceseigenaar | Afdelingsmanager/directeur |
| Naam: | Naam: |
| Functie: | Functie: |
| Datum: | Datum: |
|  |  |
| Handtekening | Handtekening |

[ ] Consultatie bij ISO/BSO uitgevoerd?

*<****Optioneel:*** *voeg hier de beoordeling van de BSO toe in de vorm van e-mail bewijs>*

**Goedkeuringen:** *<te gebruiken bij hoog risico,**verwijder indien niet van toepassing>*

|  |  |
| --- | --- |
| Systeemeigenaar/proceseigenaar | Afdelingsmanager/directeur |
| Naam: | Naam: |
| Functie: | Functie: |
| Datum: | Datum: |
|  |  |
| Handtekening | Handtekening |

[ ] Consultatie bij ISO/BSO uitgevoerd?

*<****Verplicht****: voeg hier de beoordeling van de BSO toe in de vorm van e-mail bewijs>*

*<****Optioneel****: voeg de beoordeling van de CISO toe>*

**Goedkeuringen:** *<te gebruiken bij zeer hoog risico,**verwijder indien niet van toepassing>*

|  |  |
| --- | --- |
| Systeemeigenaar/proceseigenaar | Afdelingsmanager/directeur |
| Naam: | Naam: |
| Functie: | Functie: |
| Datum: | Datum: |
|  |  |
| Handtekening | Handtekening |

<**Verplicht**: voeg hier de beoordeling van de CISO toe in de vorm van e-mail bewijs>

Faculteitsbestuur / College van Bestuur <streep door welke niet van toepassing is>

Naam:

Datum:

Handtekening