Risico Acceptatie formulier

#

# Het management moet weten dat er onbehandelde risico’s zijn

*De risicoacceptatie is een manier om bewust risico te accepteren en dat vast te leggen in een overeenkomst. Als maatregelen omtrent een risico niet meteen of helemaal niet geïmplementeerd worden, dan ontstaat er een risico dat voor kortere of langere tijd geaccepteerd moet worden door de bedrijfsvoering. Het is daarbij van belang dat de bedrijfsvoering dat risico kent, goede afwegingen maakt en bewust accepteert, en dat hiervan een audit trail (in de vorm van bewuste besluitvorming) aanwezig is. Risicoacceptatie betekent dat men zich ervan bewust is dat er risico’s zijn waar (nog) geen maatregelen tegen genomen zijn.*

*Bij een dergelijk risico moet een Risico Acceptatie Overeenkomst (RAO) worden afgesloten met de proceseigenaar of de systeemeigenaar waarna deze wordt gerapporteerd aan het College van Bestuur en opgenomen in het riskregister (vastgelegd in het ISMS). Ook als er geen RAO wordt afgesloten (bijvoorbeeld omdat risico eigenaar dit niet wil of niet bekend is), wordt daarover gerapporteerd aan het College van Bestuur. Want ook het niet hebben van een risico-eigenaar is een risico voor de organisatie. Daarnaast kan het College van Bestuur of de directie de proces- of systeemeigenaar overrulen en besluiten dat het risico niet (tijdelijk) geaccepteerd mag worden.*

|  |  |
| --- | --- |
| Aan |  |
| Van | CISO (Paul Geerts) en ISO (Miranda van der Ploeg-Cools/Tessel Stoppelenburg) |
| Afdeling | Information Security |
| CC | CIO / GRC officer |
| Datum |  |
| Onderwerp |  |
| Applicatie |  |
| Classificatie |  |
| Privacy gerelateerd? |  |
| SURF control |  |
| Geldig tot |  |
| Volgnummer |  |

#

# Inleiding

Het huidige beleid vereist het treffen van passende maatregelen ter bescherming van informatie en het systeem dat onder verantwoordelijkheid valt van <naam eigenaar/verantwoordelijke >. Binnen dit systeem, <naam systeem> is een risico aanwezig als gevolg van:

<verdere uitleg omstandigheden en risico>

Dit risico is in de volgende paragraaf verder uitgeschreven en vanuit risicomanagement wordt een advies gegeven hoe met het onderkende risico moet worden omgegaan. Zowel de proceseigenaar als het managementteam van de verantwoordelijke afdeling wordt gevraagd het voorgestelde besluit te nemen.

Dit Risico Acceptatie formulier is geldig tot de afgesproken datum en wordt in het risicoregister opgenomen. Hierna moet deze opnieuw geëvalueerd worden. In het geval van een significante wijziging in de risico's zal deze evaluatie eerder plaatsvinden.

# Beschrijving Risico

<Eigenaar/verantwoordelijke> heeft een risico als gevolg van een risicoclassificatie op een dreiging <beschrijving dreiging>:

1. Beschikbaarheid: <classificatie B>
2. Integriteit: <classificatie I>
3. Vertrouwelijkheid: <classificatie V>

<Verdere beschrijving risico>

#

# Voorgestelde oplossingen

1. <Beschrijving oplossing>
2. <Beschrijving oplossing>

# Advies

Vanuit security management wordt geadviseerd <beschrijving advies>.

# Hiermee verklaren de ondergetekenden

* Kennis te hebben genomen van het advies en de voorgestelde oplossingen.
* Het risico wordt (doorhalen wat niet van toepassing is):
	+ geaccepteerd en er worden verder geen maatregelen genomen. Maatregelen worden niet proportioneel geacht ten opzichte van het risico <aanvullen>;
	+ gemitigeerd door op de kortst mogelijke termijn de oplossing, ten uitvoering te brengen <aanvullen>;
	+ tijdelijk opgelost middels de oplossing ten uitvoering te brengen <aanvullen>.

**Motivatie bij acceptatie van het risico**

Er worden geen maatregelen genomen om het risico te mitigeren, omdat <motivatie invullen>.

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

Een afschrift van dit Risico Acceptatie formulier wordt verstrekt aan de portefeuillehouder informatiebeveiliging van het College van Bestuur.

**Advies CISO**

|  |
| --- |
| T.a.v. de keuze om het risico te accepteren/mitigeren/tijdelijk op te lossen (doorhalen wat van toepassing is) adviseert de CISO de portefeuillehouder informatiebeveiliging als volgt: |