
Comment [DK1]: Om te leren hoe dit document in te vullen zie deze **video Tutorial** "How to Write ISO 27001 Procedure for Corrective and Preventive Action"
<http://www.iso27001standard.com/tutorial/free-video-tutorial-how-to-write-iso-27001-procedure-for-corrective-action/>

Comment [DK2]: Om meer te leren over dit onderwerp, lees dit artikel: Practical use of corrective actions for ISO 27001 and ISO 22301
<http://www.iso27001standard.com/blog/2013/12/09/practical-use-of-corrective-actions-for-iso-27001-and-iso-22301/>

[logo organisatie]

Comment [DK3]: Alle velden in dit document gemarkeerd met spekhaken [] moeten worden ingevuld.

[naam organisatie]

PROCEDURE VOOR CORRIGERENDE MAATREGEL

Code:	-----
Versie:	
Versiedatum	
Gemaakt door:	
Goedgekeurd door:	
Classificatie:	

Comment [DK4]: De documentcodering moet in overeenstemming zijn met het bestaande organisatiecoderingssysteem; indien een dergelijk systeem niet is geïmplementeerd, dan kan deze regel worden verwijderd.

Versieblad

Datum	Versie	Gemaakt door	Omschrijving van de aanpassing
DD/MM/JJJJ	0.1	Dejan Kosutic	Concept Basisdocument

Inhoudsopgave

1. DOEL, TOEPASSINGSGBIED EN GEBRUIKERS	3
2. GEREFEREERDE DOCUMENTEN	3
3. CORRIGERENDE EN CORRECTIEVE MAATREGELEN	3
3.1. AFWIJKINGEN EN CORRECTIES.....	3
3.2. CORRIGERENDE MAATREGELEN	3
3.3. IMPLEMENTATIE VAN CORRIGERENDE MAATREGELEN	4
4. REGISTRATIEBEHEER OP BASIS VAN DIT DOCUMENT	4
5. GELDIGHEID EN DOCUMENTBEHEER	5
6. BIJLAGE	5

1. Doel, toepassingsgebied en gebruikers

Het doel van deze procedure is alle activiteiten met betrekking tot de initiatie, implementatie en het bijhouden van de registratie van correcties, evenals corrigerende maatregelen te beschrijven.

De procedure is van toepassing op alle activiteiten geïmplementeerd in het Managementsysteem voor Informatiebeveiliging (ISMS) [Managementsysteem voor Bedrijfscontinuïteit (BCMS)].

Gebruikers van dit document zijn alle werknemers van [naam organisatie].

Comment [DK5]: Dit moet ingevoegd worden in plaats van het ISMS in geval dat de procedure sec verwijst naar bedrijfscontinuïteitsbeheer.

2. Gerefereerde documenten

- ISO/IEC 27001 norm, clause 10.1
- ISO 22301 norm, clause 10.1
- BS 25999-2 standaard, clause 6.1
- Informatiebeveiligingsbeleid
- Bedrijfscontinuïteitsbeleid
- Procedure voor Interne Audit
- Procedure voor Incidentbeheer

Comment [DK6]: Verwijder indien de procedure alleen verwijst naar bedrijfscontinuïteitsbeheer.

Comment [DK7]: Verwijder dit indien u bedrijfscontinuïteitsbeheer niet implementeert.

Comment [DK8]: Verwijder indien de procedure alleen verwijst naar bedrijfscontinuïteitsbeheer.

Comment [DK9]: Verwijder dit indien u bedrijfscontinuïteitsbeheer niet implementeert.

Comment [DK10]: Indien de documentatie alleen is geschreven voor bedrijfscontinuïteit, vervang dan met Incidentenopvangplan.

3. Corrigerende en correctieve maatregelen

3.1. Afwijkingen en correcties

Een afwijking is elk falen om te voldoen aan de vereisten uit de normen, interne documenten, registrering, contractuele en andere verplichtingen binnen het [ISMS]. Afwijkingen kunnen worden geïdentificeerd tijdens een in- of externe audit, gebaseerd op resultaten van de directiebeoordeling na incidenten, tijdens de normale bedrijfsvoering of bij elke andere gelegenheid.

Comment [DK11]: Of BCMS

Een werknemer die een afwijking constateert dient onmiddellijk maatregelen te nemen om het te beheersen en met de gevolgen omgaan, vallen een werknemer met verantwoordelijkheid is voor een dergelijke afwijking dan dient hij/zij de informatie omtrent de afwijking door te sturen naar de verantwoordelijke die het dient te corrigeren.

3.2. Corrigerende maatregelen

Genoemde verantwoordelijke dient de behoefte te evalueren om de oorzaak van de afwijking te elimineren en herhaling te voorkomen door corrigerende maatregelen te nemen. Het belangrijkste resultaat is dat corrigerende maatregelen de oorzaak van afwijking wegvoert naar correctie afzet focust op de afwijking te beheersen en omgaan met de directe gevolgen.

Corrigerende maatregelen kunnen worden geïnitieerd door elke werknemer of (waar van toepassing) klant, leverancier of afdelingshoofd van de organisatie. Corrigerende maatregelen kunnen vereisen dat enig document, proces of regeling binnen het ISMS wordt aangepast.

Comment [DK12]: Of BCMS

3.3. Implementatie van corrigerende maatregelen

Corrigerende acties worden op de volgende manier geïmplementeerd:

Stap	Verantwoordelijke voor implementatie
1. <i>Verantwoordelijke van de afwijking</i>	Iedereen met een rol in het ISMS
2. Bepalen van de oorzaak van de afwijking	<i>Verantwoordelijke voor het gebied waar de afwijking is geïdentificeerd</i>
3. <i>Identificeren of mogelijk andere afwijkingen of tekorten</i>	Verantwoordelijke voor het gebied waar de afwijking is geïdentificeerd
4. Evalueren van de behoefte voor maatregelen om de afwijking te elimineren	<i>Verantwoordelijke voor het gebied waar de afwijking is geïdentificeerd</i>
5. Bepalen van de maatregelen die nodig zijn om de oorzaak van de afwijking te elimineren en ervoor te zorgen dat de afwijking niet meer voorkomt	Verantwoordelijke voor het gebied waar de afwijking is geïdentificeerd
6. Implementatie van de geplande maatregelen	<i>Persoon belast met de implementatie, benoemd door de verantwoordelijke</i>
7. Controleren of de genomen maatregel heeft geleid tot de eliminatie van de oorzaak van de afwijking	[functie]
8. Informeren van alle betrokkenen die een corrigerende maatregel hebben geïmplementeerd	<i>Persoon belast met de implementatie, benoemd door de verantwoordelijke</i>
9. <i>Wisselende verantwoordelijke in het ISMS, indien van toepassing</i>	Persoon die de leiding heeft over de coördinatie van het ISMS

Comment [DK13]: Of BCMS

Comment [DK14]: Eén persoon kan worden

Personen kunnen worden benoemd voor de implementatie van maatregelen tegen afwijkingen. Het is aan de verantwoordelijke voor de implementatie van maatregelen tegen afwijkingen om te bepalen welke personen hiervoor verantwoordelijk zijn.

persoon te benoemen elke keer dat een corrigerende maatregel wordt geïnitieerd.

Implementatie van maatregelen tegen afwijkingen wordt meestal gecontroleerd door de interne auditor.

Comment [DK15]: Of BCMS

Comment [DK16]: Bijv. de Informatiebeveiliging of de Coördinator Bedrijfscontinuïteit.

Comment [DK17]: Of BCMS

Elk van de bovengenoemde stappen dienen te worden vastgelegd in het **corrigerende maatregel formulier**.

Comment [DK18]: U kunt bijv. ook de

Implementatie van maatregelen tegen afwijkingen wordt meestal gecontroleerd door de interne auditor.

op te lossen.

4. Registratiebeheer op basis van dit document

Naam registratie	Opslaglocatie	Persoon verantwoordelijk voor opslag	Beveiligingsmaatregelen voor registraties	Bewaartermijn
Corrigerende maatregel	[naam of archiefmap, in	[functie]	Nadat alle gegevens zijn vastgelegd, dient elke	3 jaar

formulier	welke kast] [map op intranet]		toevoeging of wijziging te worden ontmanteld	
-----------	-------------------------------------	--	---	--

Comment [DK19]: Indien registraties worden bewaard in papieren vorm.

Comment [DK20]: Indien u een applicatie gebruikt specificeer dan de applicatienaam.

5. Geldigheid en documentbeheer

Dit document is geldig vanaf [datum].

De eigenaar van dit document is [functie]. *[Dit is slechts een document te controleren en indien nodig het minstens eens per jaar bij te werken.]*

Comment [DK21]: Dit is slechts een aanbeveling, pas de frequentie zo nodig aan.

Wanneer de doeltreffendheid en toereikendheid van dit document wordt beoordeeld, dan dienen de volgende criteria in ogenschouw te worden genomen:

- aantal geïnitieerde corrigerende en preventieve maatregelen
- aantal noodzakelijke corrigerende en preventieve maatregelen
- aantal genomen corrigerende en preventieve maatregelen zonder te hebben teruggevoerd in de aangewezen vorm

6. Bijlage

- Corrigerende Maatregel Formulier

Comment [DK22]: Verwijder dit gedeelte indien u een applicatie gebruikt.

[functie]

[naam]

[handtekening]

Comment [DK23]: Alleen noodzakelijk indien de Procedure voor Beheersing voor Documenten en Registraties een ondertekening voorschrijft.