[logo organisatie]

[naam organisatie]

PROCEDURE VOOR INTERNE AUDIT

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

Comment [DK1]: Om te leren hoe dit document in te vullen, zie deze videohandleiding "How to Write ISO 27001/ISO 22301 Internal Audit Procedure and Audit Program":
- Indien u de toolkit heeft gekocht, dan vindt u het in het ISO 27001 & ISO 22301 Klantenportaal: https://epps.customerhub.net/
- Indien u de toolkit niet heeft gekocht, dan vindt u de preview van de handleiding hier: http://www.iso27001standard.com/how-to-write-iso-27001-iso-22301-internal-audit-procedure-and-audit-program

Comment [DK2]: Om meer te leren over dit onderwerp, lees dit artikel: Dilemmas with ISO 27001 internal auditors http://www.iso27001standard.com/blog/2010/03/22/dilemmas-with-iso-27001-bs-25999-2-internal-auditors/

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

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, toepassingsgebied en gebruikers

Het doel van deze procedure is om alle auditgerelateerde activiteiten te beschrijven – schrijven van het auditprogramma, selecteren van een auditor, uitvoeren van afzonderlijke audits en rapportage.

Deze procedure is van toepassing op alle uitgevoerde activiteiten binnen het Managementsysteem voor Informatiebeveiliging (ISMS) [Managementsysteem voor Bedrijfscontinuïteit (BCMS)].

Gebruikers van dit document zijn [leden van de directie] van [naam organisatie], evenals de interne auditors.

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

Comment [DK6]: Hoogste leidinggevende instantie binnen het toepassingsgebied van het ISMS/BCMS.

2. Gerefereerde documenten

- ISO/IEC 27001 norm, clausule 9.2
- ISO 22301 norm, clausule 9.2
- BS 25999-2 standaard, clausule 5.1
- Informatiebeveiligingsbeleid
- Bedrijfscontinuïteitsbeleid
- Procedure voor Corrigerende Maatregelen

Comment [DK7]: Verwijder dit item indien de procedure alleen naar bedrijfscontinuïteitsbeheer verwijst.

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

3. Interne audit

3.1. Doel van interne audit

Het doel van interne audit is vast te stellen of procedures, beheersmaatregelen, processen, regelingen en andere activiteiten binnen het ISMS [BCMS] in overeenstemming zijn met ISO 27001 en ISO 22301 normen/BS 25999-2 standaard, geldende regelgeving, en de interne documentatie van de organisatie, of ze doeltreffend worden geïmplementeerd en onderhouden en of ze voldoen aan de beleidseisen en gestelde doelen.

Comment [DK9]: Te verwijderen indien de procedure alleen verwijst naar bedrijfscontinuïteitsbeheer.

Comment [DK10]: Te verwijderen indien u bedrijfscontinuïteitsbeheer niet zult implementeren.

3.2. Planning interne audits

[Functie] keurt een jaarlijks programma voor interne audits goed, geschreven zoals het overzicht in het formulier in Bijlage 1.

Een of meer interne audits zouden moeten worden uitgevoerd in de loop van een jaar, voor een cumulatieve dekking omgend van het hele ISMS [BCMS] toepassingsgebied. Interne audits worden gepland op basis van risicobeoordeling, evenals op resultaten van voorgaande audits, zij worden meestal uitgevoerd voor een directiebeoordeling.

Het Jaarlijkse Interne Auditprogramma zal de volgende informatie voor elke afzonderlijke interne audit moeten bevatten:

- periode van de audit (specificeer data, of maand waarin de audit gepland staat)

- toepassingsgebeid van de audit (afdelingen, processen, clausules van de norm, enz.)
- auditcriteria (normen/standaarden, wetgeving en regelgeving, interne documentatie, bedrijfsnormen, en(/of contractuele verplichtingen)
- auditmethoden (herbeoordelen van documentatie, interviews met werknemers, herbeoordeling van informatiesystemen, enz.)
- wie voert de audit uit (indien er meer dan één auditor is, specificeer dan de teamleider van de audit)

Gehouden audits moeten worden vastgelegd in het Jaarlijkse Interne Auditprogramma.

3.3. Benoemen interne auditors

[Functie]zal de interne auditors benoemen.

Een interne auditor kan iemand zijn van de organisatie of een persoon van buiten de organisatie. Criteria voor het benoemen van interne auditors zij:

- kennis van ISO/IEC 27001 en ISO 22301 normen/BS 25999-2 standaard
- bekendheid met het managementsysteem voor auditechnieken
- kennis van hoe informatie- en communicatietechnologie werken in die mate dat hij/zij bekend is met het doel van de afzonderlijke systemen evenals de gevolgen voor de beveiligingsprocessen en/of de bedrijfscontinuïteit

Comment [DK11]: Te verwijderen indien de procedure alleen verwijst naar bedrijfscontinuïteitsbeheer.

Comment [DK12]: Te verwijderen als u bedrijfscontinuïteitsbeheer niet implementeert.

Interne auditors dienen in op een zodanige manier te worden geselecteerd om te zorgen voor objectiviteit en onafhankelijkheid, d.w.z. om een conflict te vermijden omdat ze niet hun eigen werk mogen auditten.

Het is aan te bevelen dat auditors een cursus afronden voor interne auditors volgens de ISO/IEC 27001.

Comment [DK13]: Of ISO 22301/BS 25999-2.

3.4. Uitvoeren van afzonderlijke interne audits

Verantwoordelijken voor afzonderlijke interne audits worden geïdentificeerd in het Jaarlijkse Interne Auditprogramma. Indien een audit wordt uitgevoerd door een team bestaande uit verschillende auditors, dan wordt de verantwoordelijke voor de audit geïdentificeerd als Audit Teamleider.

Het volgende dient in ogenschouw te worden genomen tijdens de interne audit:

- in de in het Jaarlijkse Interne Auditprogramma neergelegde criteria
- resultaten van voorafgaande interne of externe audits
- resultaten van risicobeoordeling, invoering van maatregelen, business impact analyse, enz.
- Checklist Interne Audit – zie Bijlage 3

Het volgende dient te worden gedocumenteerd al interne autistresultaten:

- Rapport voor Interne Audit– het dient naar [functie] te worden gestuurd
- Mogelijke corrigerende maatregelen dienen te worden vastgelegd in het Formulier voor Corrigerende maatregelen, zoals vereist door de Procedure voor Corrigerende Maatregelen.

4. Registratiebeheer op basis van dit document

Naam registratie	Opslaglocatie	Persoon verantwoordelijk voor opslag	Beveiligingsmaatregelen voor registraties	Bewaartermijn
Jaarlijkse Interne Auditprogramma (in elektronische vorm)	Computer van [functie]	[functie]	Alleen [functie] en de interne auditor hebben het recht om invoer te doen en wijzigingen aan te brengen in het Jaarlijkse Interne Auditprogramma.	Programma wordt opgeslagen voor 3 jaar
Interne Audit Rapport (in elektronische vorm)	Computer van interne auditor en [functie]	Interne auditor	Rapporten worden alleen opgeslagen in alleen-lezen versies	Rapporten worden opgeslagen voor 3 jaar
Checklist Interne Audit (ingevuld formulier tijdens de interne audit)	Computer van interne auditor	Interne auditor	[De checklist wordt opgeslagen in alleen-lezen versie]	The checklist wordt opgeslagen voor de periode van 3 jaar

Comment [DK14]: Normaal de persoon die het jaarlijkse programma goedkeurt.

Comment [DK15]: Meestal in PDF-formaat.

Comment [DK16]: Meestal in PDF-formaat.

Alleen [functie] kan andere werknemers het recht van toegang verlenen tot het Jaarlijkse Interne Auditprogramma, het Rapport van Interne Audit en de Checklist Interne Audit.

5. Geldigheid en documentbeheer

Dit document is geldig vanaf [datum]

De eigenaar van dit document is [functie]. [illegible] het minstens eens per jaar bij te werken.

Comment [DK17]: 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 corrigerende maatregelen geïdentificeerd tijdens de audit
- [illegible] uitgevoerd na de interne audit

- [illegible] is met het Jaarlijkse Interne Auditprogramma

6. Bijlagen

- Bijlage 1 – Jaarlijkse Interne Auditprogramma
- Bijlage 2 – Rapport voor Interne Audit
- Bijlage 3 – Checklist Interne Audit

[functie
[naam]

_____
[handtekening]

Comment [DK18]: Alleen noodzakelijk indien de Procedure voor Beheersing voor Documenten en Registraties een ondertekening voorschrijft.