27001
Informatiebeveiliging Handleiding

ISO 27001

Bedrijfsnaam

Geautoriseerd door: Naam

Online ISO

Revisie Geschiedenis

Revisie	Datum	Wijzingen	Geaccordeerd door

Inhoudsopgave

1. Introductie

<Bedrijfsnaam> heeft een Information Security Management System (ISMS) ontwikkeld en geïmplementeerd wat het bedrijf in staat stelt om;

- Veiligheidsrisico's te beoordelen en zodanig te behandelen
- Het aantonen van toepasselijkheid aan de hand van wereldwijde standaarden
- Het laten zien aan klanten, leveranciers en belanghebbenden dat veiligheid een essentieel onderdeel is van de bedrijfsvoering
- Het beveiligen van alle financiële en vertrouwelijke data zodat de kans op ongeautoriseerde toegang zo laag mogelijk is

Deze handleiding beschrijft ons ISMS en geeft de bevoegdheden en verantwoordelijkheden weer van iedereen die hiermee werkt. Tevens refereert het naar alle procedures en activiteiten welke binnen het toepassingsgebied vallen van het ISMS.

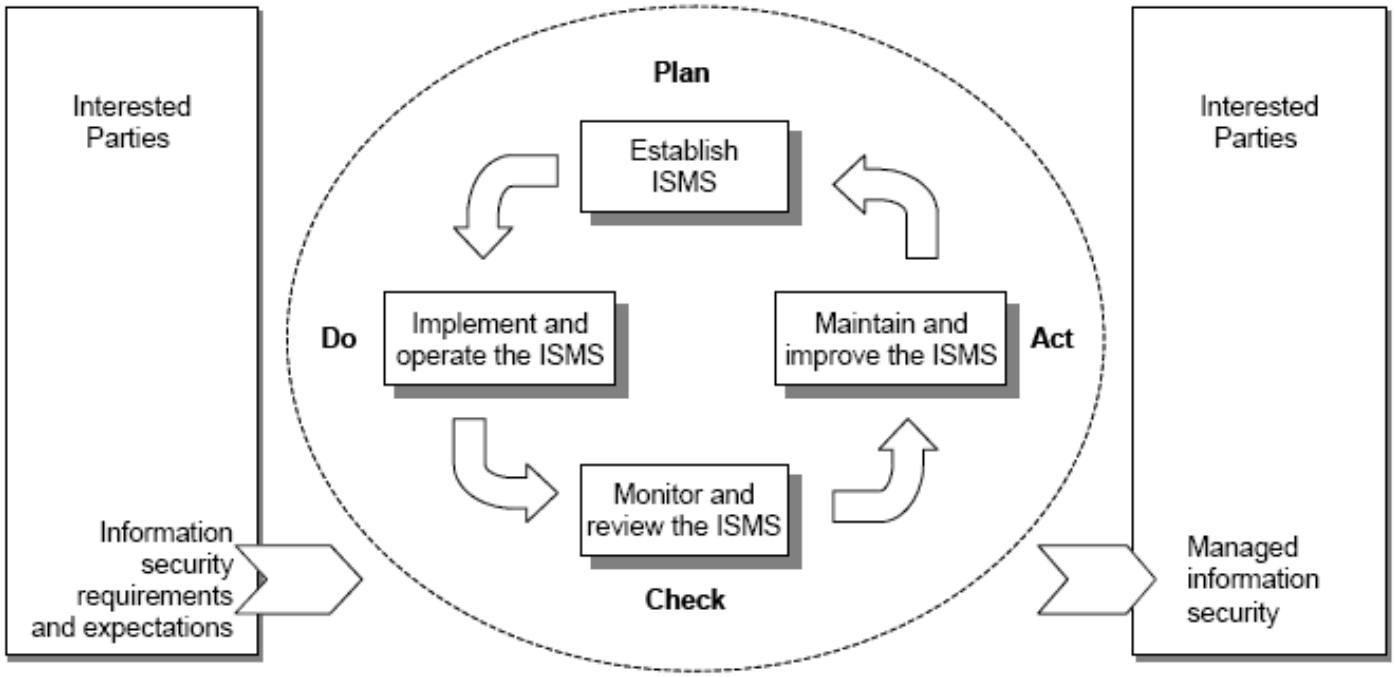
1.1 ISO 27001:2022

Ons ISMS is ontwikkeld in overeenstemming met de geldende ISO 27001:2022 standaarden welke gebaseerd zijn op een procesmatige aanpak voor het tot stand brengen, implementeren, onderhouden en continu verbeteren van ons ISMS binnen de context van de organisatie.

Het begrijpen en onderhouden van onze processen als een integraal systeem stelt ons in staat om alle relaties en afhankelijkheden te controleren om tot een algehele verbetering te komen.

Het beheren van de processen en het systeem wordt gedaan aan de hand van het Plan-Do-Check-Act principe van Deming. Deze cyclus focust op een continue risico analyse om nieuwe mogelijkheden te onderzoeken en daarbij risico's zoveel mogelijk te voorkomen of beheersen.

1.2 Plan-Do-Check-Act (PDCA) Cyclus



2. Referenties

Standaard	Titel	Beschrijving
ISO 27000:2022	Information security management systems	Update
ISO 27000:2014	Information security management systems	Overzicht en vocabulaire
ISO 27001:2013	Information security management systems	Vereisten
ISO 27002:2013	Information technology - security techniques	Gedragscode voor informatiebeveiliging
ISO 27001:2013	Auditing Management Systems	Richtlijnen voor verificatie

3. Termen en Definities

De terminologie gebruikt in deze ISMS handleiding refereert aan ISO 27001:2022 en:

- standaard bedrijfsterminologie
- termen en vocabulaire welke veel gebruikt wordt in onze industrie en markt
- termen en vocabulaire welke veel gebruikt wordt in onze standaarden en regelgeving binnen onze activiteiten en doelgroep.

Definities:

- “naleving en verplichtingen” betekent alle lokale, nationale en internationale regelgeving en vereisten welke van toepassing zijn op de organisatie. Daarnaast zijn eventuele andere verplichtingen zoals contracten, gedragsregels en standaarden van toepassing.
- “Top Management”, zoals beschreven door ISO, is vertegenwoordigd in <Bedrijfsnaam> door de <Directie>
- “personeel” iedereen die werkt in het bedrijf
- “we” en “ons” refereren naar <Bedrijfsnaam>

4. Context van de Organisatie

4.1 Inzicht verkrijgen in de organisatie en haar context

<Bedrijfsnaam> heeft meerdere externe en interne onderwerpen vastgesteld met als doel het managementsysteem voor informatiebeveiliging te behalen.

4.2 Inzicht verkrijgen in de behoeften en verwachtingen van belanghebbenden

Om een goed inzicht te krijgen in de organisatie hebben we alle belangrijke interne en externe issues geïdentificeerd weke relevant zijn op onze operatie en welke invloed hebben op ons bekwaamheid om de resultaten van het ISMS te behalen.

Dit betekent concreet:

- Het begrijpen van onze belangrijkste producten, services en processen
- Het begrijpen van het toepassingsgebied van ons ISMS
- Identificeren welke belanghebbenden relevant zijn
- Identificeren en begrijpen welke vereisten van interne en externe partijen relevant zijn

Veel van deze issues zijn geïdentificeerd na het uitvoeren van een risico analyse. Onze interne en externe issues worden gemonitord als onderdeel van het informatiebeveiliging managementsysteem en worden geüpdatet als dat nodig is.

In onze procedure **Identificeren van Informatie Beveiliging Context** wordt de gebruikte methode beschreven voor het implementeren en beheren hiervan.

In onze procedure **Naleving van wettelijke en contractuele Eisen** beschrijven en beheren we onderwerpen zoals;

- Juridisch, statutair, regelgeving of contractuele verplichting gerelateerd aan ISMS
- Beveiliging vereisten

4.3 Het toepassingsgebied van het managementsysteem voor informatiebeveiliging vaststellen

4.3.1 Toepassingsgebied

Ons managementsysteem voor informatiebeveiliging voldoet aan alle vereisten van ISO 27001:2022 en ondersteunt al onze operationele processen op kantoor voor het beheren en documenteren van onze operationele processen op het hoofdkantoor en alle andere locaties. Het ontwerpen, ontwikkelen, produceren, installeren en onderhouden van onze producten wordt hierin meegenomen en is gebaseerd op het begrijpen van onze bedrijfsvoering en de verwachtingen van belanghebbenden.

Voeg hier uw toepassingsgebied verklaring toe. Deze verklaring moet de activiteiten, producten en services beschrijven die van toepassing zijn op het ISMS in één enkele zin. Indien je ervoor kiest om een externe audit te laten uitvoeren voor certificatie, dan zal deze samenvatting weergegeven worden op het ISO 27001:2022 certificaat.

De <Directie> moet het toepassingsgebied van de ISMS implementatie vaststellen aan de hand van de scope welke men wil beschermen. Dit is een belangrijke stap in het ISO proces en moet met zorg gekozen worden waarbij geen details worden overgeslagen.

Bijvoorbeeld, als het bedrijf gebruikt maakt van mobiele telefoons dan zullen deze hoogstwaarschijnlijk gevoelige informatie bevatten. Als deze apparaten toegang hebben tot het beveiligde netwerk zullen deze toegevoegd moeten worden aan het toepassingsgebied.

Indien je besluit om over te gaan tot certificatie, zal de auditor toetsen of alle elementen zoals beschreven in het toepassingsgebied juist zijn geïmplementeerd in het ISMS. Elementen of afdelingen welke zijn uitgesloten van het toepassingsgebied zullen niet beoordeeld worden.

Samengevat, ISO 27001 beschrijft de volgende vereisten voor het vaststellen van het toepassingsgebied:

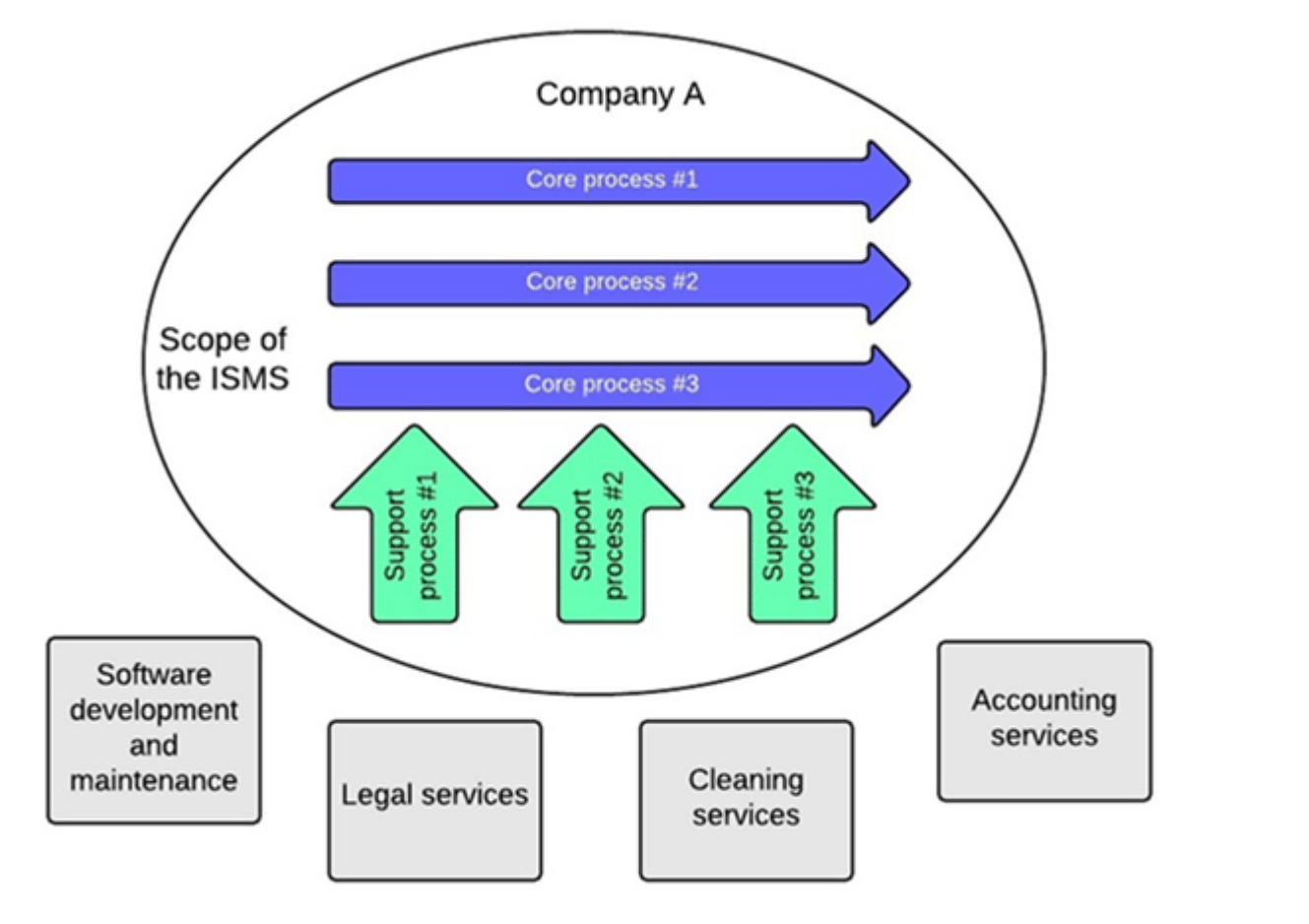
- *Interne en externe issue gedefinieerd in clausule 4.1 worden in acht genomen*
- *Vereisten gedefinieerd in clausule 4.2 worden in acht genomen*
- *Overweeg afhankelijkheden tussen de ISMS scope en externen in acht te nemen*

Niet vereist maar wellicht wel zinvol is het toevoegen van een korte beschrijving van je locatie en operationele afdelingen indien je een bepaalde ruimte of groep wil uitsluiten van de scope.

4.3.2 Afhankelijkheden

Voor het beschrijven van afhankelijkheden is het zinvol een diagram te maken waarin de bedrijfsprocessen visueel worden weergegeven welke binnen het toepassingsgebied vallen. Buiten dit diagram kunnen dan de externe processen of afhankelijkheden worden aangegeven en hun impact op de organisatie.

In het geval je al ISO 9001 hebt geïmplanteerd, heb je waarschijnlijk al een soortgelijke proces diagram:



Zodra de afhankelijkheden bekend zijn moeten de interfaces worden geïdentificeerd. Zodra deze bekend beschreven zijn inclusief hun in- en output kunnen ze worden opgenomen in het toepassingsgebied voor het ISMS.

4.3.3 Voorbeeld Toepassingsgebied 27001

Ons managementsysteem voor informatiebeveiliging beschrijft alle bedrijven, kantoren en resources binnen de <Kantoorlocatie>. Kantoren en resources buiten de <Kantoorlocatie> zijn uitgesloten van het ISMS toepassingsgebied.

Ons ISMS toepassingsgebied omvat alle bedrijfsprocessen van de IT Afdeling geleid door de < IT Manager>. Alle andere bedrijfsprocessen zijn uitgesloten van het ISMS toepassingsgebied.

Ons ISMS beschermt de vertrouwelijkheid, integriteit en beschikbaarheid van <Bedrijfsnaam> klanten data ten alle tijden op ons <Kantoorlocatie> kantoor. Dit is inclusief de IT afdeling, klant contactcenters en <Kantoorlocaties>.

Bij het vaststellen van het toepassingsgebied zijn de volgende punten overwogen:

- Onze organisatie en zijn context (interne en externe issues)
- De eisen en verwachtingen van belanghebbenden
- De interfaces en afhankelijkheden tussen onze eigen activiteiten en die welke door externen worden uitgevoerd.

4.3.4 Uitsluitingen

De volgende elementen zijn niet van toepassing op onze bedrijfsvoering en uitgesloten van het ISMS:

Uitsluitingen	Reden voor Uitsluiting
Thuiswerken (A.6.2) (Voorbeeld)	Thuiswerken is momenteel niet toegestaan en daardoor niet opgenomen in het toepassingsgebied

De volgende fysieke locaties of ruimtes worden uitgesloten van de ISMS scope:

Locatie/ruimte	Reden voor Uitsluiting
Magazijn	
Kantoor Amsterdam	

4.4 Managementsysteem voor Informatiebeveiliging

Om onze informatiebeveiliging doelstellingen te behalen hebben we dit ISMS opgezet en geïmplementeerd en deze wordt continue onderhouden en verbeterd aan de hand van onze beschreven bedrijfsprocessen.

Ons ISMS houdt hierbij rekening met de eisen en verwachtingen van (externe) belanghebbenden.

5. Leiderschap

5.1 Leiderschap en betrokkenheid

De directie toont leiderschap en betrokkenheid om de doelstellingen van ons ISMS te behalen door verantwoordelijkheid te nemen voor de effectiviteit van het ISMS en door:

- Het opzetten van informatiebeveiliging procedure en informatiebeveiliging doelstellingen in lijn met de strategie en context van de organisatie.
- De informatiebeveiliging vereisten zijn degelijk geïntegreerd in onze bedrijfsprocessen
- Voldoende resources toe te kennen aan het onderhouden van het ISMS
- Duidelijk te communiceren over het belang en de waarde van een goed functioneren informatiebeveiliging managementsysteem en bijbehorende vereisten
- Ervoor te zorgen dat de beoogde resultaten daadwerkelijk behaald worden
- Het personeel te motiveren bij te dragen aan de effectiviteit van het managementsysteem
- Het promoten van continu verbeteren
- De informatiebeveiligingen procedures ook een onderdeel te maken van de individuele verantwoordelijkheden en prestatie doelen

5.2 Beleid

De directie heeft een informatiebeveiligingsbeleid opgesteld met als doel:

“Het opzetten, monitoren en continue verbeteren van onze beveiliging op het gebied van vertrouwelijkheid, integriteit en beschikbaarheid van fysieke en elektronische informatie om ervoor te zorgen dat aan regelgeving en contractuele vereisten wordt voldaan”

Dit beleid beschrijft de dagelijkse operatie om de communicatie en implementatie van informatiebeveiliging binnen de organisatie te waarborgen. Ons informatiebeveiliging beleid is beschikbaar gesteld als document en verspreidt binnen het bedrijf ter kennisgeving.

Het informatiebeveiliging beleid wordt elk jaar vernieuwd als onderdeel van de informatiebeveiliging Directiebeoordeling. Indien het nodig blijkt om deze tussentijds te updaten zal dat zodanig gedaan worden om tegemoet te komen aan de eisen en verwachtingen van belanghebbenden of indien nieuwe risico’s geïdentificeerd worden door het risico beheersproces.

5.3 Rollen, verantwoordelijkheden en bevoegdheden binnen de organisatie

De <Directie> heeft verschillende verantwoordelijkheden en autorisaties toegewezen voor het implementeren, opereren en beheren van het ISMS. Inclusief;

Verantwoordelijkheid	Primair Verantwoordelijk
Vaststellen van het toepassingsgebied van het managementsysteem voor informatiebeveiliging inclusief context, strategie, beleid en Directiebeoordeling.	<Directie>
Draagvlak en focus creëren voor informatiebeveiliging binnen de organisatie	<Directie>, <ISMS Manager>, <IT Manager>
Opstellen van ISMS doelen en plannen	<Directie>, <ISMS Manager>, <IT Manager>
Controleren van ISMS documenten	<Document Beheerder>
Controleren van ISMS registraties	<Document Beheerder>
Informatiebeveiliging training, bewustzijn en competentie	<HR Manager> en <ISMS Manager>
Beheren van interne ISMS audits	<Audit Manager>
Corrigerende en preventieve maatregelen	<ISMS Manager>
Assessment en behandelen van informatiebeveiliging risico's	<ISMS Manager> en risico eigenaren
Het zeker stellen dat het ISMS voldoet aan de geldende standaarden	<ISMS Manager>
Implementeren, opereren, monitoren, beoordelen, onderhouden en verbeteren van het ISMS	<ISMS Manager>
De integriteit van het ISMS onderhouden en het doorvoeren van geplande changes	<ISMS Manager.
Het organiseren van onafhankelijke informatiebeveiliging beoordelingen binnen het bedrijf	<ISMS Manager> en <Audit Manager>
Het opzetten en onderhouden van de nodige beschermende maatregelen om de operationele assets te beveiligen	<ISMS Manager>
Het beschermen van personeel informatie	<HR Manager> en <ISMS Manager>
Fysieke en omgevingsbeveiliging	<Facilitair Manager> en <ISMS Manager>

Communicatie en operations management	<ISMS Manager>
Media berichtgeving en informatie uitwisseling	<ISMS Manager>
Netwerk beveiliging management en toegangsbeheer	<ISMS Manager>
Acquisitie, ontwikkeling en onderhoud van informatiesystemen	<IT Manager>, <Inkoop Manager>, <ISMS Manager>
Informatiebeveiliging incident management	<ISMS Manager>
Bedrijfscontinuïteit management	<ISMS Manager>
Voldoen aan juridische regelgeving omtrent informatiebeveiliging	<ISMS Manager>
Voldoen aan contractuele verplichtingen omtrent informatiebeveiliging	<Sales Manager> en <ISMS Manager>

Deze verantwoordelijkheden en autorisaties zijn goed gecommuniceerd binnen de organisatie en zijn ook beschreven in de functieprofielen.

Van alle manager wordt verwacht dat zij een bepaalde mate van toewijding laten zijn bij de ontwikkeling en verbetering van het ISMS door:

- het toewijzen van de nodige resources
- betrokkenheid bij het interne audit proces
- proactieve houding waarbij continue verbeteren voorop staat
- focus op verbetering van operationele processen

Alle managers zijn verantwoordelijk voor het implementeren van het beleid, processen en system zoals beschreven in deze handleiding. Zij plannen, informeren en sturen de resources binnen hun afdeling volgens het algemeen geldende ISMS.

Al het personeel is verantwoordelijk voor de implementeren van het beleid en bijbehorende procedures die van toepassing zijn op hun werkgebied. Tevens worden zijn aangemoedigd om potentiele problemen te identificeren en rapporteren met daarbij een aanbevolen gerelateerde oplossing.

6. Planning

6.1 Maatregelen om risico's te beperken en kansen te benutten

Bij het opstellen van ons ISMS, zijn risico's en kansen geïdentificeerd welke overwogen moeten worden om in de hoofdstukken 4.1 *Inzicht verkrijgen in de organisatie en haar context* en 4.2 *Inzicht verkrijgen in de behoeften en verwachtingen van belanghebbenden*. De risico's en kansen worden vastgesteld om;

- te bewerkstelligen dat ons managementsysteem voor informatiebeveiliging het beoogde resultaat behaald
- ongewenste effecten te voorkomen en te beperken;
- continue verbetering te bereiken

Bij het beheren van de kansen en risico's hebben we een risico behandel assessment procedure opgezet welke veiligheidsrisico criteria beschrijft en beheerd inclusief de risico acceptactie criteria en de criteria voor het uitvoering van informatiebeveiliging risico assessments.

- Risico's en kansen worden bij het implementeren en onderhouden van het ISMS overwogen
- Niet elke risico zal een formeel risico management processen kunnen ondergaan en daarom wordt het risiconiveau in alle gevallen afgezet tegen de te nemen acties
- De te nemen maatregelen om risico's te mitigeren worden zijn altijd in lijn met de potentiele impact op de informatiebeveiliging.

Het identificeren, beoordelen, evalueren en behandelen van informatiebeveiliging risico's en kansen wordt gedaan en beheerd in onze **Beheersen van Risico's en Kansen Procedure**

6.2 Informatiebeveiligingsdoelstellingen en de planning om ze te bereiken

6.2.1 Algemeen

De <Directie> heeft informatiebeveiligingsdoelstellingen vastgesteld om

- Zeker te zijn dat we de voortgang van de operatie kunnen waarborgen met minimale onderbrekingen
- Integriteit te waarborgen voor alle informatie welke we verspreiden of produceren
- Alle informatie met voldoende vertrouwelijkheid te behandelen
- Informatiebeveiliging training toe te voegen aan ons introductie proces
- Informatiebeveiliging incidenten te beperken tot maximaal 4 per jaar

Deze informatiebeveiligingsdoelstellingen zijn gebaseerd op de vereisten en risico's die gedefinieerd zijn in het ISMS.

De <Directie> waarborgt dat de informatiebeveiligingsdoelstellingen;

- consistent zijn en in lijn met onze informatiebeveiligingsbeleid
- meetbaar zijn
- worden gemonitord
- gecommuniceerd zijn
- worden geüpdatet wanneer nodig

De voortgang om deze doelen te bereiken worden beoordeeld tijdens het informatiebeveiliging management review overleg door de <Directie> en de <ISMS Manager>.

Deze doelen en de resultaten van dit overleg worden gecommuniceerd aan alle werknemers, klanten, leveranciers, aannemers en belanghebbenden.

Elke informatiebeveiligingsdoelstelling wordt gedocumenteerd en onderhouden in het ISMS. Wanneer een proces niet voldoet aan de doelstelling of wanneer er onverwachts een probleem optreed in een proces wordt de procedure **Beheer van Corrigerende en Preventieve Acties Rapportering (CPAR)** in werking gesteld om de situatie te onderzoeken en het probleem op te lossen. Vervolgens wordt gekeken of het proces verbeterd kan worden.

6.2.2 *Maatregelen plannen voor het bereiken van informatiebeveiligingsdoelstellingen*

Bij het maken van een plan om de informatiebeveiligingsdoelstellingen te bereiken, stellen we het volgende vast;

- wat er gedaan dient te worden
- welke resources benodigd zijn
- wie er verantwoordelijk is
- wanneer het zal worden voltooid
- hoe de resultaten zullen worden geëvalueerd, inclusief indicatoren voor het monitoren van de voortgang in het bereiken van onze meetbare doelstellingen voor informatiebeveiliging.

Indien mogelijk zullen we naar opties zoeken om de Informatiebeveiligingsdoelstellingen te integreren in de operationele processen.

Periodiek, of wanneer de Informatiebeveiligingsdoelstellingen wijzigen, zal de <ISMS Manager> het **Informatiebeveiligingsdoelstellingen Plan** voorbereiden en voorleggen aan de <Directie> ter goedkeuring voor uitvoering.

6.3 Verander Management

Deze handleiding beschrijft ons plan voor het uitvoeren, onderhouden en verbeteren van ons ISMS.

Indien veranderingen doorgevoerd moeten worden in een van onze bedrijfsprocessen, zullen deze worden gepland, uitgevoerd en gevalideerd worden volgens de **Beheer van managementsysteem Documentatie Procedure**

Onze informatiebeveiliging Directiebeoordeling en interne audit processen waarborgen de continue integriteit van het ISMS wanneer significante veranderen zijn gepland.

7. Ondersteuning

7.1 Middelen

7.1.1 Algemeen

De <Directie> zorgt dat alle nodige middelen beschikbaar zijn om;

- Het ISMS te implementeren en te onderhouden
- Continue verbeteringen door te voeren voor effectiviteit

Het inzetten en toewijzen van resources wordt beoordeeld en gemonitord tijdens de informatiebeveiliging Directiebeoordeling.

7.2 Competentie

Voeg hier uw eventuele competentie regelingen toe

7.3 Bewustzijn

Voeg hier uw eventuele bewustzijn regelingen toe

7.4 Communicatie

We opereren en onderhouden verscheidene regelingen om de competentie, bewustzijn en communicatie te waarborgen.

Deze regelingen zorgen ervoor dat;

- Alle werknemers zijn competent om hun eigen taken uit te voeren
- Alle werknemers zijn op de hoogte van;
  - Onze management systemen en de gerelateerde beleidsprocedures en doelen
  - Hun eigen rol en verantwoordelijkheid
  - Het belang van hun eigen bijdragen aan de werking van de management systemen
  - De voordelen van hun eigen verbeteringen in prestatie
  - De belangrijkheid om aan het management systeem, beleid en procedures te voldoen
  - De consequenties wanneer niet aan een management systeem, beleid of procedures wordt voldaan
  - Wat te doen in geval van nood
  - Veranderingen van het management systeem
  - De resultaten van de jaarlijkse Directiebeoordeling van het management systeem met betrekking tot hun eigen doelstellingen
- Training behoeftes bekend zijn
- Degelijke training plannen worden ontwikkeld en uitgevoerd (met de <HR Manager>)
- Elke rol wordt beschreven in het **Functiebeschrijving Register**

Naast onze eigen werknemers worden er ook bewustzijn campagnes opgezet voor het informeren van aannemers, tijdelijke uitzendkrachten, bezoekers en andere belanghebbenden.

7.5 Documenten en Registraties

7.5.1 Algemeen

Onze ISMS documentatie set bestaat uit “Documenten” en “Registraties”. ISO 27001:2022 gebruikt alleen de term “Gedocumenteerde informatie” maar ons managementsysteem maakt een onderscheid tussen een “document” en “registratie” om verwarring te voorkomen. We beschouwen een “document” als een geschreven informatie stuk om een bepaalde activiteit te beschrijven en een “registratie” wordt gebruikt om het resultaat van invoering te bewijzen van een bepaalde activiteit.

De <Directie> heeft de omvang van de gedocumenteerde informatie vastgesteld door middel van;

- Vereist door de ISO 27001:2022 International Standard
- Nodig voor de effectiviteit van ons eigen ISMS

Dit is gebaseerd op de volgende criteria;

- De omvang van ons bedrijf
- Het toepassingsgebied, complexiteit en interactie tussen de processen en producten/services
- De vraag naar het aantonen
- De noodzaak om aan te tonen dat we aan alle nalevingsverplichtingen voldoen
- De competentie van ons personeel

7.5.2 Creëren en actualiseren

Onze documentatie set is opgezet en wordt beheerd door middel van ons kwaliteit managementsysteem zoals beschreven in **Beheer van managementsysteem Documentatie Procedure**.

Dit management system zorgt ervoor dat onze werknemers ten alle tijden toegang hebben tot de laatste geaccordeerde versie van openbaar gemaakte documenten

7.5.3 Beheer van registraties

Het identificeren, opslaan, ophalen, beschermen, archiveren, en verspreiden van gegevens is beschreven in **Beheer van managementsysteem Registraties Procedure.** Deze procedure beschrijft ook de methode voor het beheren van de registraties welke gemaakt zijn door onze leveranciers.

8. Uitvoering

8.1 Operationele planning en beheersing

De <Directie> is verantwoordelijk voor het implementeren van de processen volgens de ISMS vereisten om risico's en kansen te adresseren en om informatiebeveiliging doelstellingen te plannen en beheren.

- we identificeren, beoordelen en behandelen onze informatiebeveiliging risico's en kansen in onze **Beheersen van Risico's en Kansen Procedure**
- de <ISMS Manager>, bereidt periodiek, of wanneer informatiebeveiliging doelstellingen tussentijds veranderen, een **Informatiebeveiligingsdoelstellingen Plan** voor welke wordt voorgelegd aan de <Directie> ter goedkeuring, implementatie en monitoring.
- Voor zover nodig houden, analyseren en evalueren we gegevens om erop te kunnen vertrouwen dat de processen worden uitgevoerd zoals initieel gepland
- we beheersen geplande changes en evalueren de consequenties van onverwachtse changes door de effecten te mitigeren als dat nodig blijkt te zijn
- we beheersen processen welke we hebben uitbesteed aan aannemers zoals beschreven in **Beheer van Uitbestede Processen Procedure**
- indient een proces niet leidt tot het gestelde doel of er treed een tussentijds probleem op wordt ons beleid **Beheer van Corrigerende en Preventieve Acties Rapportering (CPAR)** Procedure geactiveerd om het probleem te onderzoeken en op te lossen. Indien nodig verbeteren we achteraf het proces.
- We beoordelen de geschiktheid, toereikendheid en effectiviteit van dit managementsysteem, in overeenstemming met onze **Beheer van de Directiebeoordeling** Procedure

  Deze beoordelingen omvatten het beoordelen van de voortdurende afstemming van ons ISMS op onze strategische richting, mogelijkheden voor verbetering en de noodzaak van veranderingen

8.2 Risicobeoordeling van informatiebeveiliging

De <Directie> waarborgt dat periodiek en indien nodig risicobeoordelingen van informatiebeveiliging worden uitgevoerd. De resultaten worden genotuleerd en opgeslagen.

Deze risicobeoordelingen zijn gebaseerd op onze risicobeoordelingscriteria en wordt beschreven in **Beheersen van Risico's en Kansen Procedure.**

8.3 Informatiebeveiligingsrisico’s behandelen

We beheren en controleren onze risico’s zoals beschreven in **Beheersen van Risico’s en Kansen Procedure**

9. Evaluatie van de prestaties

9.1 Monitoren, meten, analyseren en evalueren

Om de prestaties van ons ISMS te evalueren, bepalen we:

- wat moet worden beheerd en gemeten
- de methoden voor monitoring, meting, analyse en evaluatie die nodig zijn om geldige resultaten te garanderen
- de criteria waaraan we onze informatiebeveiligingsprestaties en verschillende indicatoren evalueren
- wanneer dergelijke monitoring en meting moet worden uitgevoerd
- wanneer de resultaten van monitoring en meting geanalyseerd en geëvalueerd moeten worden

Deze activiteiten worden gebruikt om te evalueren:

- de prestaties en effectiviteit van ons ISMS
- de effectiviteit van de genomen maatregelen om risico's en kansen aan te pakken
- de effectiviteit van planning
- de prestaties van externe leveranciers
- andere verbeteringen aan het managementsysteem

We beheren en onderhouden regelingen voor deze monitoring, meting, analyse en evaluatie zoals uiteengezet in onze **Beheer van monitoring, meting, analyse en evaluatie procedure**.

9.2 Interne Audit

We werken en onderhouden regelingen voor de interne audit met geplande tussenpozen zoals uiteengezet in onze **Beheer van de interne audit Procedure.**

Door middel van deze audits verstrekken we informatie aan het management en bepalen we of ons ISMS:

- voldoet aan onze eigen eisen
- voldoet aan de eisen van de ISO 27001
- effectief wordt geïmplementeerd en onderhouden
- effectief is in het bereiken van het beleid en de doelstellingen van ons managementsysteem

9.3 Directiebeoordeling

We maken en onderhouden regelingen voor de beoordeling van de geschiktheid, toereikendheid en effectiviteit van ons ISMS, met geplande tussenpozen zoals uiteengezet in onze **Beheer van de Directiebeoordeling Procedure**.

Deze beoordelingen omvatten het beoordelen van de voortdurende afstemming van ons ISMS op onze strategische richting, mogelijkheden voor verbetering en de noodzaak van veranderingen

10. Verbetering

10.1 Algemeen

We gebruiken ons ISMS en andere input om onze resultaten op het gebied van informatiebeveiliging continu te verbeteren.

De verbetermogelijkheden die we zoeken zijn onder meer:

- inspelen op veranderende en toekomstige behoeften en verwachtingen
- corrigeren, voorkomen en verminderen van ongewenste effecten
- het verbeteren van de prestaties en effectiviteit van ons ISMS

10.2 Afwijkingen en corrigerende maatregelen

We werken en onderhouden regelingen om corrigerende maatregelen te nemen om de oorzaak van non-conformiteit te elimineren en verder te voorkomen, en preventieve maatregelen om de oorzaken van mogelijke vergelijkbare non-conformiteiten te elimineren, zoals uiteengezet in onze **Beheer van Corrigerende en Preventieve Acties Rapportering (CPAR) Procedure.**

10.3 Continue verbetering

We proberen de geschiktheid, toereikendheid en effectiviteit van ons ISMS voortdurend te verbeteren.

We gebruiken de resultaten van de analyse en evaluatie, en de resultaten van de informatiebeveiliging Directiebeoordeling, om behoeften en kansen voor een dergelijke verbetering te identificeren.

De algehele effectiviteit van ons programma van voortdurende verbetering, met inbegrip van zowel corrigerende maatregelen als onze bredere voortgang bij het bereiken van doelstellingen voor verbetering op bedrijfsniveau, wordt bewaakt en beoordeeld via ons **Beheer van de Directiebeoordeling Procedure.**

Bijlage A

We passen informatie beheersdoelstellingen en beheersmaatregelen toe zoals uiteengezet in bijlage A van ISO 27001: 2022 en voegen waar nodig aanvullende beheersdoelstellingen en beheersmaatregelen toe.

We hebben onze aanpak van de beheersdoelstellingen en beheersmaatregelen uiteengezet in bijlage A in onze beheerdoelstellingen en beheersmaatregelen documenten:

- **A5 Organisatorische Maatregelen**
- **A6 Mensen**
- **A7 Fysieke Maatregelen**
- **A8 Technologische Maatregelen**

We beschrijven de operationele beleidstukken en procedures die nodig zijn om de consistente toepassing van de juiste bewaking op alle activiteiten en systemen binnen de scope van ons ISMS te waarborgen.

Appendix 1 - Organigram

Voeg hier het organigram van de organisatie toe

Appendix 2 - High Level Proces Overzicht

Voeg hier het high-level proces overzicht toe van de organisatie waarin alle geïdentificeerde processen worden weergegeven inclusief de afhankelijkheden.