[logo organisatie]

[naam organisatie]

INFORMATIEBEVEILIGINGSBELEID

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

Comment [DK1]: Om te leren hoe dit document in te vullen, zie:

1) **Video tutorial** 'How to Write the ISMS Policy According to ISO 27001' http://www.iso27001standard.com/tutorial/free-video-tutorial-how-to-write-the-iso-27001-information-security-policy/

Comment [DK2]: Dit artikel zal u helpen te begrijpen wat het doel is van het Informatiebeveiligingsbeleid: Information security policy – how detailed should it be? http://www.iso27001standard.com/blog/2010/05/26/information-security-policy-how-detailed-should-it-be/

Comment [DK3]: Indien u een document nodig heeft dat gedetailleerde regels levert voor informatiebeveiliging, gebruik dan a.u.b. the Verklaring van Aanvaardbaar Gebruik opgenomen in de toolkit.

Hier kunt u los de Verklaring van Aanvaardbaar Gebruik kopen: http://www.iso27001standard.com/documentation/acceptable-use-policy/

Comment [DK4]: Alle velden in dit document gemarkeerd met spekhaken [ ] moeten worden ingevuld.

Comment [DK5]: De documentcodering moet in overeenstemming zijn met het bestaande organisatie coderingssysteem; 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

Dit top-level Beleid is gericht op het definiëren van het doel, de richting, de principes en de basisregels voor Informatiebeveiliging.

Dit Beleid is van toepassing op het gehele Managementsysteem voor Informatiebeveiliging (ISMS), als bepaald in het Document Toepassingsgebied ISMS.

Gebruikers van dit document zijn zowel alle werknemers van [naam organisatie], als ook de relevante externe partijen.

2. Gerefereerde documenten

- ISO/IEC 27001 norm, clausule 5.2 en 5.3
- Document Toepassingsgebied ISMS
- Methodologie voor Risicobeoordeling en Risicobehandeling
- Verklaring van Toepasselijkheid
- Lijst van Wet-, Regelgeving, Contractuele en Andere Verplichtingen
-
- [Bedrijfscontinuïteitsbeleid]
- [Procedure voor Incidentbeheer]

Comment [DK6]: Maak een lijst van andere interne documenten die geassocieerd worden met dit Beleid - bijvoorbeeld, strategisch ontwikkelingsplan, bedrijfsplan, document aangaande strategisch risicobeheer, enz.

Comment [DK7]: Zie paragraaf 4.4

Comment [DK8]: Zie paragraaf 4.5

3. Basisterminologie Informatiebeveiliging

Vertrouwelijkheid - [illegible] personen of systemen.

Integriteit – [illegible] worden gewijzigd door bevoegde personen of systemen.

Beschikbaarheid – kenmerk van de informatie dat de informatie beschikbaar is voor bevoegde personen als de informatie nodig is.

Informatiebeveiliging - [illegible] informatie

Managementsysteem voor Informatiebeveiliging – deel van het gehele managementproces dat zorg [illegible] informatiebeveiliging.

4. Beheersen van de Informatiebeveiliging

4.1. Doelstellingen en metingen

Algemene doelen voor het managementsysteem voor informatiebeveiliging zijn de volgende: het [illegible] bedrijfsplannen van de organisatie.[Functie] is verantwoordelijk voor het herbeoordelen van de bestaande doelen van het ISMS en het stellen van nieuwe.

Comment [DK9]: Indien nodig, verander en/of [illegible] gebruikerstevredenheid, enz.

Doelstellingen voor afzonderlijke beveiligingsmaatregelen of groepen van maatregelen worden [illegible] [functie] in de Verklaring van Toepasselijkheid.

Al deze doelstellingen moeten minstens één keer per jaar worden herbeoordeeld.

Comment [DK10]: Beoordeel of deze frequentie van toepassing is.

[Naam organisatie] zal meten in hoeverre alle doestellingen zijn behaald. [Functie] is [illegible] meetresultaten analyseren en evalueren en rapporteren aan het [top management] als input voor de Directiebeoordeling.

4.2. Eisen informatiebeveiliging

Dit beleid en het hele ISMS dienen in overeenstemming te zijn met de in de wet- en regelgeving [illegible] ook met de contractuele verplichtingen.

Comment [DK11]: Maak ook een lijst voor [illegible] gegevens, bedrijfscontinuïteit, bescherming persoonsgegevens, enz.

[illegible] in de Lijst van Wet-, Regelgeving, Contractuele en Andere Verplichtingen.

4.3. Beheersmaatregelen informatiebeveiliging

[illegible] wordt bepaald in de Methodologie voor Risicobeoordeling en Risicobehandeling.

De geselecteerde beheersmaatregelen en hun implementiestatus worden getoond in de Verklaring van Toepasselijkheid.

4.4. Bedrijfscontinuïteit

Comment [DK12]: Verwijder deze paragraaf [illegible] geïmplementeerd.

[illegible]

4.5. Verantwoordelijkheden

Basisverantwoordelijkheden voor het ISMS zijn:

- [functie] is verantwoordelijk voor het waarborgen van het volgens dit Beleid implementeren [illegible] noodzakelijke middelen

Comment [DK13]: Lid van de directie.

- [functie] is verantwoordelijk voor zowel de operationele coördinatie van het ISMS als ook voor de rapportage over het ISMS
- [directie] dient minstens één keer per jaar het ISMS te herbeoordelen of elke keer wanneer zich significante wijzigingen voordoen en stelt notulen op naar aanleiding van die vergadering. Het doel van de directieherbeoordeling is om de geschiktheid, toereikendheid en doeltreffendheid van het ISMS vast te stellen.
- [functie] implementeert training- en bewustwordingsprogramma's voor medewerkers op het gebied van informatiebeveiliging
- de bescherming van de integriteit, beschikbaarheid en vertrouwelijkheid van bedrijfsmiddelen is de verantwoordelijkheid van de eigenaar van elke bedrijfsmiddel
- alle beveiligingsincidenten of zwakke punten moeten worden gemeld aan [functie]
- [Functie] zal bepalen welke informatie, gerelateerd is aan informatiebeveiliging, zal worden gecommuniceerd naar welke derde partij (zowel intern en extern), bij wie en wanneer.
- [Functie] is verantwoordelijk voor het overnemen en implementeren van het Plan voor Training en Bewustzijn welke voor alle personen geldt die een rol hebben binnen Informatiebeveiligingsmanagement.

Comment [DK14]: Een of meerdere personen; verantwoordelijkheden kunnen worden toegewezen volgens aanvullende ISMS-aspecten.

Comment [DK15]: Dit moet het directieorgaan zijn in het ISMS toepassingsgebied - bv. raad van bestuur, directie, enz.

Comment [DK16]: Verschillende verantwoordelijkheden kunnen worden toegewezen, volgens de soorten incidenten.

Comment [DK17]: Of maak een verwijzing naar de Procedure voor Incidentbeheer.

4.6. Communicatie Beleid

[Functie] dient te waarborgen dat zowel alle werknemers van [naam organisatie], als ook alle van toepassing zijnde externe partijen die een rol hebben in het ISMS, dit Beleid kennen.

5. Ondersteuning bij de implementatie van het ISMS

Hierbij verklaart [functie of het directieorgaan uit het toepassingsgebied van het ISMS] dat alle fasen in de implementatie van het ISMS en continue verbetering zullen worden ondersteund met adequate middelen om alle doelen en doelstellingen van dit Beleid te realiseren, als ook aan alle geïdentificeerde eisen te voldoen.

6. Geldigheid en documentbeheer

Dit document is geldig vanaf [datum]

De eigenaar van dit document is [functie]. Hij/zij dient het document te controleren en indien nodig het minstens één keer per jaar bij te werken.

Comment [DK18]: Dit is slechts een aanbeveling, zie de frequentie is nodig om

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

- het aantal werknemers en externe partijen die een rol hebben in het ISMS, maar dit document niet kennen
- niet-naleving van het ISMS met de wetten en regels, contractuele verplichtingen, en andere interne documenten van de organisatie

- ineffectiviteit van de implementatie en het onderhoud van het ISMS
- [illegible]

[functie]
[naam]

Comment [DK19]: Het Beleid moet worden goedgekeurd door de directie uit het toepassingsgebied van het ISMS.

_____

[handtekening]

Comment [DK20]: Alleen noodzakelijk indien de Procedure voor Beheersing van Documenten en Registraties voorschrijft dat papieren documenten moeten worden ondertekend.