Beschrijving van de generieke norm:

ISO 27001:2013

Grafimedia en Creatieve Industrie

Versie: augustus 2016

Uitgave van de Stichting Certificatie Grafimedia branche (SCGM)

Stichting Certificatie GrafiMedia

INHOUDSOPGAVE

INHOUDSOPGAVE 1
INLEIDING 4
1. ONDERWERP EN TOEPASSINGSGEBIED 6
2. NORMATIEVE VERWIJZINGEN 6
3. TERMEN EN DEFINITIES 6
3.1 Termen met betrekking tot organisatie en leiderschap 6
3.2 Termen met betrekking tot planning 6
3.3 Termen in verband met ondersteuning en uitvoering 7
3.4 Termen met betrekking tot het evalueren en verbeteren van prestaties 7
4. CONTEXT VAN DE ORGANISATIE 7
4.1 Inzicht in de Organisatie en haar context 7
4.2 Inzicht in de behoeften en verwachtingen van belanghebbenden 7
4.3 Het toepassingsgebied van het managementsysteem 8
4.4 Managementsysteem 8
5. LEIDERSCHAP 8
5.1 Leiderschap en betrokkenheid 8
5.1.1 Algemeen 8
5.1.2 Stakeholdergerichtheid 9
5.2 Beleid 9
5.2.1 Het beleid vaststellen 9
5.2.2 Het beleid kenbaar maken 9
5.3 Rollen, verantwoordelijkheden en bevoegdheden binnen de organisatie 9
6. Planning 9
6.1 Acties om risico's en kansen op te pakken 10
6.1.1 Algemeen 10
6.1.2 Risicobeoordeling van specifieke normaspecten 10
6.1.3 Behandelen van Risico's en verplichtingen 11
6.1.4 Acties plannen 11
6.2 Doelstellingen en de planning om ze te bereiken 11
6.2.1 Doelstellingen 11
6.2.2 Acties plannen om de doelstellingen te bereiken 12
6.3 Planning van wijzigingen 12
7. Ondersteuning ..... **Fout! Bladwijzer niet gedefinieerd.**
7.1 Middelen 12
7.1.1 Algemeen 12
7.1.2 Personeel 12
7.1.3 Infrastructuur 12
7.1.4 Omgeving voor de uitvoering van processen 13
7.1.5 Middelen voor monitoring en meting 13
7.1.6 Kennis binnen de organisatie 13
7.2 Competentie 14
7.3 Bewustzijn 14
7.4 Communicatie 14
7.4.1 Algemeen 14
7.4.2 Interne communicatie 14
7.4.3 Externe communicatie 14
7.5 Gedocumenteerde informatie 14
7.5.1 Algemeen 14
7.5.2 Creëren en actualiseren 15
7.5.3 Beheersing van gedocumenteerde informatie 15
8. Uitvoering ..... **Fout! Bladwijzer niet gedefinieerd.**
8.1 Operationele planning en beheersing 15

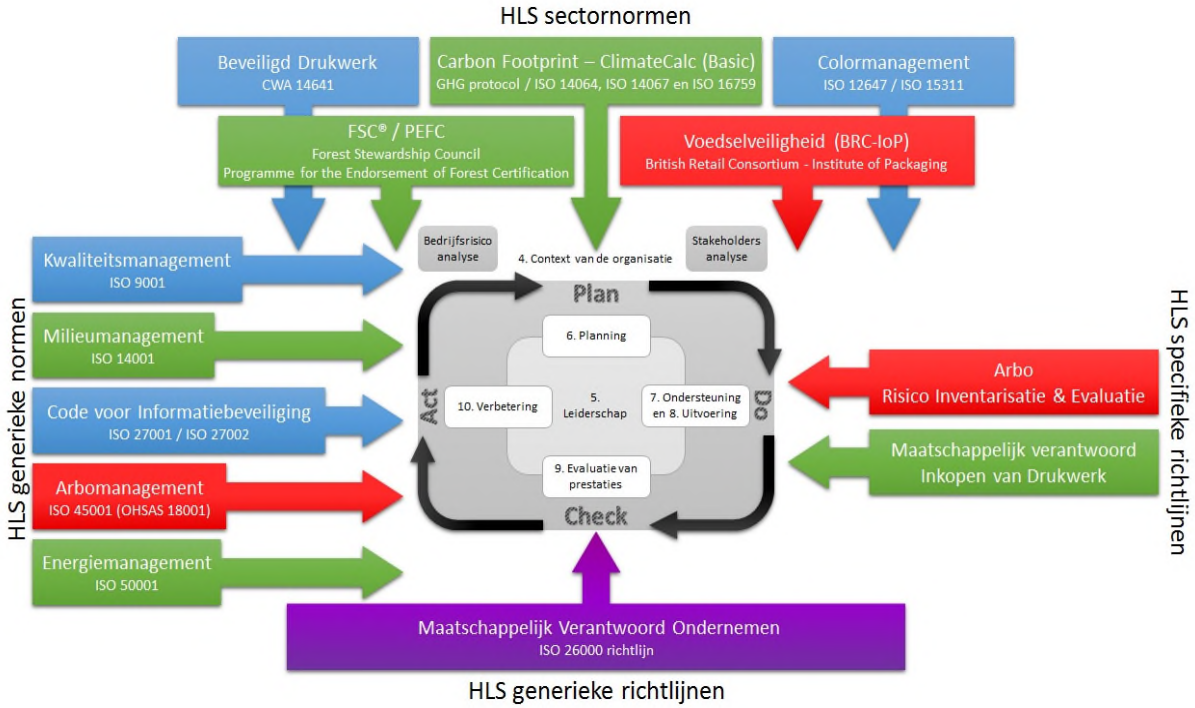
8.2 Eisen voor producten en diensten en processen 15
8.2.1 Communicatie met de stakeholder 15
8.2.2 Het vaststellen van de eisen voor producten, diensten en processen 15
8.2.3 Beoordeling van de eisen voor producten en diensten en processen 16
8.2.4 Wijzigingen in eisen voor producten en diensten en processen 16
8.3 Ontwerp en ontwikkeling van producten, diensten 16
8.3.1 Algemeen 16
8.3.2 Planning van ontwerp en ontwikkeling 16
8.3.3 Inputs voor ontwerp en ontwikkeling 16
8.3.4 Beheersmaatregelen voor ontwerp en ontwikkeling 16
8.3.5 Ontwerp- en ontwikkelingsoutputs 16
8.3.6 Wijzigingen met betrekking ontwerp en ontwikkeling 16
8.4 Beheersing van extern geleverde processen, producten en diensten 17
8.4.1 Algemeen 17
8.4.2 Soort en mate van beheersing 17
8.4.3 Informatie voor externe aanbieders 17
8.5 Productie en het leveren van diensten 17
8.5.1 Beheersing van de productie en het leveren van diensten 17
8.5.2 Identificatie en naspeurbaarheid 17
8.5.3 Eigendom van klanten of externe aanbieders 17
8.5.4 In stand houden 17
8.5.5 Nazorgactiviteiten 17
8.5.6 Beheersing van wijzigingen 18
8.6 Vrijgave van producten en diensten 18
8.7 Beheersing van afwijkingen 18
9. Evaluatie van de prestaties ..... **Fout! Bladwijzer niet gedefinieerd.**
9.1 Monitoren, meten, analyseren en evalueren 18
9.1.1 Algemeen 18
9.1.2 Stakeholder tevredenheid 18
9.1.3 Analyse en evaluatie 18
9.2 Interne audit 18
9.2.1 Algemeen 18
9.2.2 Intern auditprogramma 19
9.3 Directiebeoordeling 19
9.3.1 Algemeen 19
9.3.2 Inputs voor directiebeoordeling 19
9.3.3 Outputs van directiebeoordeling 19
10. Verbetering ..... **Fout! Bladwijzer niet gedefinieerd.**
10.1 Algemeen 20
10.2 Afwijkingen en corrigerende maatregelen 20
10.3 Continue verbetering 20

INLEIDING

Dit document bevat de 'generieke norm ISO 27001:2013'. Een generieke norm is een aanvulling op de zogenaamde High Level Structure. De combinatie van een generieke norm en die High Level Structure (HLS) maakt een volledige, certificeerbare norm. Dit is omschreven in de 'HLS leeswijzer Grafimedia en Creatieve Industrie' (gratis te downloaden via de website van SCGM).

In de HLS leeswijzer Grafimedia en Creatieve Industrie leest u meer over deze werkwijze en over de indeling van documenten. Er is namelijk een vaste hoofdstukindeling, waardoor u andere inhoudelijke thema's – bijvoorbeeld kwaliteitsmanagement – ISO 9001:2015 – en milieumanagement – ISO 14001:2015 – op dezelfde wijze kan benaderen. Dit moet het voor organisaties makkelijker maken om meerdere systemen te integreren.

In de HLS leeswijzer Grafimedia en Creatieve Industrie vindt u ook het volgende schema:



Schematische weergave van het zogenaamde plug-in-model van de HLS. De HLS vormt het bedrijfskundig managementsysteem, waaraan de verschillende normen of specifieke richtlijnen zijn vastgeklikt.

U ziet dat het Code voor Informatiebeveiliging (ISO 27001) als HLS generieke norm op een bedrijfskundig managementsysteem 'inplugt'. Hier ziet u ook de inhoudelijke hoofdstukken van de HLS én de generieke ISO 27001:2013 terug, die ook in dit document gevolgd wordt.

In de generieke norm ISO 27001:2013 vindt u het volgende terug. De eerste drie hoofdstukken zijn van algemene aard en derhalve minder relevant.

1. Onderwerp & toepassingsgebied *(= de inleiding van de kwaliteitsnorm*)
2. Normatieve verwijzingen *(= welke specifieke norm wordt gebruikt*)
3. Termen en definities (= *geeft uitleg over diverse technische woorden*)
4. Context van de organisatie (= *vanuit welke drive opereert de organisatie t.a.v. kwaliteit*)
5. Leiderschap (= *verantwoordelijkheid nemen en rolverdeling*)
6. Planning (= *inventariseren, evalueren en plannen)*
7. Ondersteuning (= *de succesbepalende voorwaarden voor kwaliteitszorg in de bedrijfsvoering*)

8. Uitvoering (= *beheersing van de werkzaamheden in alle relevante processen*)
9. Evaluatie van de prestaties (= *meting, interne auditing en directiebeoordeling*)
10. Verbetering (= *continue verbetering van de prestaties*)

De HLS leeswijzer Creatieve Industrie beschrijft de basisinvulling van de eisen waaraan u moet voldoen indien u een certificeerbaar ISO-certificeerbaar managementsysteem wilt invoeren en handhaven. De generieke norm ISO 27001 beschrijft, per hoofdstuk en paragraaf, onder het kopje '**Informatiebeveiliging'** de specifieke aanvullende eisen vanuit ISO 27001:2013.

Bijvoorbeeld: normparagraaf 4.1 is voor alle ISO normen 'Inzicht in de Organisatie en haar context'. Dit onderwerp is voor elke norm relevant. U haalt de relevante eisen uit de Leeswijzer HLS en dit document dat u nu leest.

Voor sommige generieke normen zijn er (sub)paragrafen die de HLS niet heeft. In dat geval is er alleen een eis vanuit de generieke norm. Voor de internationale ISO normen geldt dat een kleine groep paragrafen niet inhoudelijk hetzelfde thema behandelen. Binnen de SCGM is dit gecorrigeerd: alle paragrafen gaan inhoudelijk over hetzelfde onderwerp. Hierdoor leest u in enkele gevallen een verwijzing naar een andere paragraaf.

De Raad van Toezicht van de SCGM hoopt dat u met deze generieke norm ISO 27001:2013 goed in staat bent een effectief en waarde toevoegend kwaliteitsmanagementsysteem in te voeren en te handhaven.

1. ONDERWERP EN TOEPASSINGSGEBIED

Informatiebeveiliging
Deze norm is zo opgesteld dat bedrijven – die een managementsysteem hebben ingevoerd dat aan de norm voldoet – consequent de volgende zaken blijven borgen en kunnen aantonen:

- De organisatie weet op een adequate wijze de risico's die horen bij informatiebeveiliging inzichtelijk te maken en adequaat te beheersen;
- De organisatie draagt zorg voor het systematisch naleven van alle relevante wet- en regelgeving aangaande dit onderwerp, in relatie tot haar stakeholders (compliance);
- Het bedrijf bereikt haar doelstellingen voor informatiebeveiliging.

Deze norm is niet alleen van toepassing op de organisatie en de activiteiten, producten en diensten die ze direct kan beheersen of beïnvloeden, maar ook op de invloed die ze in de levenscyclus (c.q. productieketen) kan uitoefenen.

Bedrijven in de Creatieve Industrie hebben ten aanzien van veel andere MKB-branches altijd informatiebeveiliging als aandachtspunt omdat ze intellectueel eigendom (en/of informatie) van klanten bewerken en verrijken (en dus moeten beschermen). Hierdoor kunnen ze snel in aanraken komen met wetgeving, die voor informatiebeveiliging sterk veranderlijk is.

2. NORMATIEVE VERWIJZINGEN

Informatiebeveiliging
De in dit document beschreven module ISO 27001:2013, welke samen met de Leeswijzer HLS de ISO 27001:2013 norm Grafimedia en Creatieve Industrie vormt, bouwt normatief verder op de *ISO 27001:2005 Informatietechnologie – Beveiligingstechnieken – Managementsystemen voor informatiebeveiliging – eisen*. Een op naam van (een actieve medewerker van) de organisatie gestelde kopie van deze officiële ISO-norm dient in de organisatie aanwezig te zijn, welke opvraagbaar is bij de NEN. Tevens wordt van de organisatie verwacht dat zij in het bezit is van de HLS Leeswijzer Grafimedia en Creatieve Industrie, op basis waarvan de organisatie haar in te voeren en te handhaven systeem op kan afstemmen.

3. TERMEN EN DEFINITIES

De officiële ISO-normen (kunnen) verwijzen naar een losstaande norm voor termen en begrippen (de '0' van de norm: bijvoorbeeld 9000:2015 Grondbeginselen en verklarende woordenlijst). Alle termen en definities zijn geplaatst in de HLS-leeswijzer Grafimedia en Creatieve Industrie. Hieronder vindt u een korte beschrijving – geen eis – hoe u de termen toe kunt passen.

3.1 Termen met betrekking tot organisatie en leiderschap

Deze termen helpen u bij:
- Het interpreteren van hoe de leiding zich verhoudt tot een organisatiestructuur en de norm;
- De definitie van wat een belanghebbende (oftewel) stakeholder is.

Dit zijn met name hoofdstuk 4 en 5.

3.2 Termen met betrekking tot planning

Deze termen helpen u bij:
- Juist interpreteren van de essentiële doelstelling van de module;