ICS: 35.040

Geregistreerde Belgische norm

NBN ISO/IEC 27001 NL

1e uitg., juli 2014

Normklasse: Z 07

Informatietechnologie - Beveiligingstechnieken - Managementsystemen voor informatiebeveiliging - Eisen (ISO/IEC 27001:2013)

Technologies de l'information - Techniques de sécurité - Systèmes de management de la sécurité de l'information - Exigences (ISO/IEC 27001:2013)

Information technology - Security techniques - Information security management systems - Requirements (ISO/IEC 27001:2013)

Toelating tot publicatie: 25 juli 2014

Deze norm ISO/IEC 27001:2013 heeft de status van een Belgische norm.

Deze norm bestaat in twee officiële versies (Engels, Frans).

De Nederlandstalige versie is uitgegeven onder de verantwoordelijkheid van het NBN. Deze NBN ISO/IEC 27001 NL is identiek aan de NBN ISO/IEC 27001, 1e uitg. juni 2014 en heeft dezelfde status als de officiële versies.

Hoewel de grootste zorg is besteed aan deze Nederlandstalige uitgave, kunnen fouten en onvolledigheden niet geheel worden uitgesloten. Het NBN kan dan ook niet aansprakelijk worden gesteld voor rechtstreekse en/of onrechtstreekse schade, ontstaan door of verband houdend met de toepassing van deze uitgave.

standards for .be

Bureau voor Normalisatie - Jozef II-straat 40 - 1000 Brussel - België
Tel: +32 2 738 01 11 - Fax: +32 2 733 42 64 - E-mail: info@nbn.be - NBN Online: www.nbn.be
Bank 679-0000951-78 IBAN BE69 6790 0009 5178 BIC PCHQBEBB BTW BE0880857592

Prijsgroep: 28

ICS: 35.040

norme belge enregistrée

NBN ISO/IEC 27001 NL

1e éd., juillet 2014

Indice de classement: Z 07

Technologies de l'information - Techniques de sécurité - Systèmes de management de la sécurité de l'information - Exigences (ISO/IEC 27001:2013)

Informatietechnologie - Beveiligingstechnieken - Managementsystemen voor informatiebeveiliging - Eisen (ISO/IEC 27001:2013)

Information technology - Security techniques - Information security management systems - Requirements (ISO/IEC 27001:2013)

Autorisation de publication: 25 juillet 2014

La présente norme ISO/IEC 27001:2013 a le statut d'une norme belge.

La présente norme existe en deux versions officielles (anglais, français).

La version en néerlandais est publiée sous la responsabilité du NBN. Cette norme NBN ISO/IEC 27001 NL est identique à la NBN ISO/IEC 27001, 1e éd. juin 2014 et a le même statut que les versions officielles.

Bien que le plus grand soin ait été apporté à la réalisation de cette édition néerlandaise, des erreurs ou omission ne peuvent être totalement exclues. Par conséquent, le NBN décline toute responsabilité pour les dommages directs et/ou indirects dus ou liés à l'application de la présente norme.

standards for .be

Bureau de Normalisation - rue Joseph II 40 - 1000 Bruxelles - Belgique
Tél: +32 2 738 01 11 - Fax: +32 2 733 42 64 - E-mail: info@nbn.be - NBN Online: www.nbn.be
Banque 679-0000951-78 IBAN BE69 6790 0009 5178 BIC PCHQBEBB TVA BE0880857592

Prix: groupe 28

Nationaal voorwoord

De internationale norm ISO/IEC 27001:2013 werd door het Bureau voor Normalisatie (NBN) ongewijzigd geregistreerd en gepubliceerd als Belgische norm.

De Nederlandstalige versie van deze norm is opgesteld door het Nederlands Normalisatie-instituut (NEN).

Deze NBN-versie is grotendeels gebaseerd op de NEN-versie, maar houdt tegelijk rekening met een aantal verschillen op het vlak van terminologie tussen Nederland en Vlaanderen. De onderstaande synoniemenlijst vermeldt de termen waarvoor het NBN een afwijkende keuze heeft gemaakt.

Synoniemenlijst

Engelse term	***Nederlandse term in de NEN-versie***	***Nederlandse term in de NBN-versie***
amendments	wijzigings- en correctiebladen	corrigenda en amendementen
information security risk treatment	behandeling van informatiebeveiligingsrisico's	aanpak van informatiebeveiligingsrisico's
information security risk treatment plan	behandelplan voor informatiebeveiligingsrisico's	plan voor de aanpak van informatiebeveiligingsrisico's
operations security	beveiliging bedrijfsvoering	beveiliging van bedrijfsactiviteiten

(blanco)

INTERNATIONALE NORM

ISO/IEC 27001

2e uitgave
2013-10-01

Informatietechnologie - Beveiligingstechnieken – Managementsystemen voor informatiebeveiliging - Eisen

Information technology - Security techniques - Information security management systems - Requirements

Technologies de l'information - Techniques de sécurité - Systèmes de management de la sécurité de l'information - Exigences

Referentienummer
ISO/IEC 27001:2013 (N)

(blanco)

Inhoud

Voorwoord

ISO (International Organization for Standardization) en IEC (International Electrotechnical Commission) vormen tezamen een stelsel dat gespecialiseerd is in wereldwijde normalisatie. Nationale organisaties die lid zijn van ISO of IEC participeren in het ontwikkelen van Internationale Normen via technische commissies die door de desbetreffende organisatie zijn ingesteld ten behoeve van de normalisatie in specifieke technische werkvelden. Technische commissies van ISO en IEC werken samen bij onderwerpen waarin zij een gemeenschappelijk belang hebben. Andere internationale organisaties, zowel overheidsinstanties als ngo's nemen, in samenwerking met ISO en IEC, ook deel aan deze werkzaamheden. Op het gebied van informatietechnologie hebben ISO en IEC een gezamenlijke technische commissie opgericht, ISO/IEC JTC 1.

Internationale Normen worden opgesteld in overeenstemming met de voorschriften die zijn opgenomen in de ISO/IEC-richtlijnen, deel 2.

De belangrijkste taak van de gezamenlijke technische commissie (JTC) is het opstellen van Internationale Normen. Ontwerpversies van Internationale Normen die zijn aangenomen door de gezamenlijke technische commissie, worden ter stemming voorgelegd aan de normalisatie-instellingen. Publicatie als Internationale Norm vereist goedkeuring van ten minste 75 % van de door nationale normalisatie-instellingen uitgebrachte stemmen.

Er wordt op gewezen dat sommige delen van dit document mogelijk beschermd zijn door patentrechten. ISO en IEC zijn niet verantwoordelijk voor identificatie van dergelijke patentrechten.

ISO/IEC 27001 is opgesteld door ISO/IEC JTC 1, *Information technology*, SC 27, *IT Security techniques*.

Deze tweede versie herroept en vervangt de eerste versie (ISO/IEC 27001:2005), die technisch is herzien.

0 Inleiding

0.1 Algemeen

Deze Internationale Norm is opgesteld om te voorzien in eisen voor het vaststellen, implementeren, bijhouden en continu verbeteren van een managementsysteem voor informatiebeveiliging. Het invoeren van een managementsysteem voor informatiebeveiliging is voor een organisatie een strategische beslissing. Het vaststellen en implementeren van een managementsysteem voor informatiebeveiliging wordt beïnvloed door de behoeften en doelstellingen van de organisatie, de beveiligingseisen, de procedures die de organisatie toepast en de omvang en structuur van de organisatie. Er wordt van uitgegaan dat al deze beïnvloedende factoren mettertijd wijzigen.

Het managementsysteem voor informatiebeveiliging beschermt de vertrouwelijkheid, de integriteit en de beschikbaarheid van informatie door een risicobeheerproces toe te passen, en geeft belanghebbenden het vertrouwen dat risico's adequaat worden beheerd.

Het is belangrijk dat het managementsysteem voor informatiebeveiliging deel uitmaakt van en geïntegreerd is met de procedures van de organisatie en met de algehele managementstructuur, en dat informatiebeveiliging in aanmerking wordt genomen bij het ontwerpen van processen, informatiesystemen en beheersmaatregelen. Er wordt van uitgegaan dat de implementatie van een managementsysteem voor informatiebeveiliging in omvang wordt afgestemd op de behoeften van de organisatie.

Deze Internationale Norm kan worden gebruikt door interne en externe partijen om het vermogen van de organisatie te beoordelen om te voldoen aan de eigen informatiebeveiligingseisen.

De volgorde waarin de eisen in deze Internationale Norm worden gepresenteerd geeft niet de volgorde van belangrijkheid aan en impliceert niet de volgorde waarin ze moeten worden geïmplementeerd. De nummering van de lijstitems dient alleen voor referentiedoeleinden.

ISO/IEC 27000 beschrijft het overzicht en de terminologie van managementsystemen voor informatiebeveiliging, en verwijst naar de normenfamilie betreffende managementsystemen voor informatiebeveiliging (met inbegrip van ISO/IEC 27003 [2], ISO/IEC 27004 [3] en ISO/IEC 27005 [4]), met gerelateerde termen en definities.

0.2 Compatibiliteit met andere managementsysteemnormen

Deze Internationale Norm past de hoofdstructuur (HLS) toe, identieke paragraaftitels, identieke tekst, gemeenschappelijke termen en kerndefinities zoals gedefinieerd in bijlage SL van ISO/IEC Directives, deel 1, geconsolideerd ISO-supplement, en is daardoor compatibel met andere managementsysteemnormen die bijlage SL hebben aangenomen.

Deze gemeenschappelijke benadering zoals gedefinieerd in bijlage SL is nuttig voor organisaties die ervoor kiezen een enkel managementsysteem uit te voeren dat voldoet aan de eisen van twee of meer managementsysteemnormen.

Informatietechnologie – Beveiligingstechnieken – Managementsystemen voor informatiebeveiliging – Eisen

1 Onderwerp en toepassingsgebied

Deze Internationale Norm noemt de eisen voor het binnen de context van de organisatie vaststellen, implementeren, bijhouden en continu verbeteren van een managementsysteem voor informatiebeveiliging. In deze Internationale Norm zijn ook eisen opgenomen voor het beoordelen en de aanpak van informatiebeveiligingsrisico's afgestemd op de behoeften van de organisatie. De eisen die in deze Internationale Norm zijn vermeld zijn algemeen en bedoeld toepasselijk te zijn voor alle organisaties, ongeacht type, omvang of aard. Als een organisatie conformiteit met deze Internationale Norm claimt, is uitsluiting van een van de eisen genoemd in de hoofdstukken 4 tot en met 10 niet acceptabel.

2 Normatieve verwijzingen

De volgende documenten, waarnaar als geheel of voor een onderdeel, in dit document normatief is verwezen, zijn onmisbaar voor de toepassing ervan. Bij gedateerde verwijzingen is alleen de aangehaalde uitgave van toepassing. Bij ongedateerde verwijzingen is de laatste uitgave van het document (met inbegrip van eventuele corrigenda en amendementen) waarnaar is verwezen van toepassing

ISO/IEC 27000, *Information technology – Security techniques – Information security management systems – Overview and vocabulary*

3 Termen en definities

Voor de toepassing van dit document gelden de termen en definities zoals vermeld in ISO/IEC 27000.

4 Context van de organisatie

4.1 Inzicht verkrijgen in de organisatie en haar context

De organisatie moet externe en interne onderwerpen vaststellen die relevant zijn voor haar doelstelling en die haar vermogen beïnvloeden om het (de) beoogde resulta(a)t(en) van haar managementsysteem voor informatiebeveiliging te behalen.

OPMERKING Het vaststellen van deze onderwerpen verwijst naar het vaststellen van de externe en interne context van de organisatie zoals behandeld in 5.3 van ISO 31000:2009 [5].

4.2 Inzicht verkrijgen in de behoeften en verwachtingen van belanghebbenden

De organisatie moet vaststellen:

a) welke belanghebbenden relevant zijn voor het managementsysteem voor informatiebeveiliging, en

b) welke eisen van deze belanghebbenden relevant zijn voor informatiebeveiliging.

OPMERKING De eisen van belanghebbenden kunnen eisen op het gebied van wet- en regelgeving en contractuele verplichtingen inhouden.