ÍST EN ISO/IEC 27001:2017

ÍSLENSKUR STAÐALL

STAÐLARÁÐ ÍSLANDS

Gildistaka 2017-04-20
ICS 29.240.01

Upplýsingatækni
– Öryggisaðferðir
– Stjórnunarkerfi um upplýsingaöryggi
– Kröfur

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

1. prentun.

Eftirtaldir aðilar styrktu útgáfu þessa staðals á íslensku:

Advania

Borgun

Capacent

Fjármálaeftirlitið

Íslandsbanki

Landhelgisgæsla Íslands

Landsbankinn

Landslög

Landsspítali

Nasdaq verðbréfamiðstöð hf

Netorka hf

Nova

Opin kerfi hf

Orkufjarskipti

Orkuveita Reykjavíkur

Persónuvernd

Reykjavíkurborg

Ríkisskattstjóri

Síminn

Sjóvá

Tollstjóri

Tryggingamiðstöðin

Veritas Capital

Vodafone

Þekking hf

Þjóðskrá Íslands

ÍST EN ISO/IEC 27001:2017

Formáli íslensku þýðingarinnar

Þessi íslenski staðall, ÍST EN ISO/IEC 27001:2013, sem einnig er evrópskur og alþjóðlegur staðall, var staðfestur af Staðlaráði Íslands, sem er samstarfsvettvangur íslenskra hagsmunaaðila til að vinna að stöðlun og beitingu staðla. Íslenska þýðingin var gerð að tilhlutan Staðlaráðs Íslands og Fagstaðlaráðs í upplýsingatækni (FUT).

Vinnuhópinn skipuðu:
- Þorvarður Kári Ólafsson formaður
- Elísabet Árnadóttir
- Grímur Kjartansson
- Guðbjörn Sverrir Hreinsson
- Jón Kristinn Ragnarsson
- Ólafur Róbert Rafnsson
- Pétur S. Hilmarsson

Þessi staðall kemur í stað ÍST ISO/IEC 27001:2005.

Þýðingin er gerð til hagræðis fyrir íslenska notendur. Kappkostað hefur verið að hafa íslenska textann eins nákvæman eins og framast er unnt. Engu að síður getur Staðlaráð Íslands ekki ábyrgst að þýðingin endurspegli nákvæmlega merkingu frumtextans, orð fyrir orð.

Af þessum sökum er enski textinn birtur við hlið hins íslenska og til hans ber að leita komi til deilumála um túlkun ákvæða í staðlinum. Staðlarnir eru í stöðugri endurskoðun og þar með þýðingin. Notendur staðlanna eru eindregið hvattir til að koma athugasemdum og ábendingum til Staðlaráðs Íslands.

EVRÓPSKUR STAÐALL
EUROPEAN STANDARD
NORME EUROPÉENNE
EUROPÄISCHE NORM

EN ISO/IEC 27001

Febrúar 2017

ICS 03.100.70, 35.030

Íslensk útgáfa

Upplýsingatækni – Öryggisaðferðir – Stjórnunarkerfi um upplýsingaöryggi – Kröfur (ISO/IEC 27001:2013 með Leiðréttingu 1:2014 og Leiðréttingu 2:2015)

Information technology – Security techniques – Information security management systems – Requirements (ISO/IEC 27001:2013 including Cor 1:2014 and Cor 2:2015)

Technologies de l'information – Techniques de sécurité – Systèmes de management de la sécurité de l'information – Exigences (ISO/IEC 27001:2013 y compris Cor 1:2014 et Cor 2:2015)

Informationstecnik – Sicherheitsverfahren – Informationssicherheits-Managementsysteme – Anforderungen (ISO/IEC 27001:2013 einschließlich Cor 1:2014 und Cor 2:2015)

Þessi staðall er hin íslenska útgáfa evrópska staðalsins EN ISO/IEC 27001:2017. Hann var þýddur af Staðlaráði Íslands. Hann hefur sama gildi og opinberu útgáfurnar.

Þessi evrópski staðall var samþykktur af CEN 26. janúar 2017.

Meðlimir CEN og CENELEC eru skyldugir til að uppfylla þær kröfur starfsreglna CEN/CENELEC sem greina frá skilyrðum þess að þessi evrópski staðall sé gerður að landsstaðli án nokkurra breytinga. Hægt er að fá nýjustu lista og skráningartilvísanir sem varða slíka landsstaðla með því að biðja um slíkt hjá aðalskrifstofunni eða hjá hvaða CEN eða CENELEC meðlim sem er.

Þessi evrópski staðall er til í þremur opinberum útgáfum (ensku, frönsku og þýsku). Útgáfa á öðru tungumáli, þar sem meðlimur CEN eða CENELEC þýðir yfir á sitt tungumál á eigin ábyrgð og tilkynnir um útgáfuna til aðalskrifstofunnar, hefur sama gildi og opinberu útgáfurnar.

Meðlimir CEN og CENELEC eru landsstaðlaráð Austurríkis, Belgíu, Búlgaríu, Danmerkur, Eistlands, Finnlands, Frakklands, Grikklands, Hollands, Írlands, Íslands, Ítalíu, Króatíu, Kýpur, Lettlands, Litháen, Lúxemborgar, Makedóníu, Möltu, Noregs, Póllands, Portúgals, Rúmeníu, Serbíu Slóvakíu, Slóveníu, Spánar, Stóra-Bretlands, Sviss, Svíþjóðar, Tékklands, Tyrklands, Ungverjalands og Þýskalands.

EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION
EUROPÄISCHES KOMITEE FÜR NORMUNG

Aðalskrifstofa: Avenue Marnix 17
B - 1000 Brussels

ÍST EN ISO/IEC 27001:2017

Formáli evrópska staðalsins

Texti ISO/IEC 27001:2013 að meðtöldum Leiðréttingu 1:2014 og Leiðréttingu 2:2015 var saminn af tækninefndinni ISO/IEC/JTC 1 „Information technology“ (Upplýsingatækni) sem heyrir undir Alþjóða staðlasamtökin (ISO) og Alþjóða raftækniráðið (IEC), og hefur verið tekinn upp sem EN ISO/IEC 27001:2017.

Þessi evrópski staðall skal fá gildi landsstaðals, annaðhvort með útgáfu alsams texta eða með staðfestingu upprunalegu útgáfunnar, í síðasta lagi fyrir lok ágúst 2017, og landsstaðlar sem innihalda kröfur sem stangast á við kröfur þessa staðals skulu jafnframt felldir úr gildi í síðasta lagi fyrir lok ágúst 2017.

Athygli er vakin á því að sum atriði í þessum alþjóðastaðli gætu fallið undir einkaleyfi. CEN og/eða CENELEC bera ekki ábyrgð á að greina einhver eða öll slík einkaleyfi.

Samkvæmt starfsreglum CEN/CENELEC eru landsstaðlastofnanir eftirtalinna landa skyldug til að innleiða þennan evrópska staðal: Austurríki, Belgía, Búlgaría, Danmörk, Eistland, Finnland, Frakkland, Grikkland, Holland, Írland, Ísland, Ítalía, Króatía, Kýpur, Lettland, Litháen, Lúxemborg, Makedónía, Malta, Noregur, Pólland, Portúgal, Rúmenía, Serbía, Slóvakía, Slóvenía, Spánn, Stóra-Bretland, Sviss, Svíþjóð, Tékkland, Tyrkland, Ungverjaland og Þýskaland.

Yfirlýsing um samþykkt:

Texti ISO/IEC 27001:2013 að meðtöldum Leiðréttingu 1:2014 og Leiðréttingu 2:2015 var samþykktur óbreyttur af CEN sem EN ISO/IEC 27001:2017.

European foreword

The text of ISO/IEC 27001:2013 including Cor 1:2014 and Cor 2:2015 has been prepared by Technical Committee ISO/IEC JTC 1 "Information technology" of the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) and has been taken over as EN ISO/IEC 27001:2017.

This European Standard shall be given the status of a national standard, either by publication of an identical text or by endorsement, at the latest by August 2017, and conflicting national standards shall be withdrawn at the latest by August 2017.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CEN [and/or CENELEC] shall not be held responsible for identifying any or all such patent rights.

According to the CEN-CENELEC Internal Regulations, the national standards organizations of the following countries are bound to implement this European Standard: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.

Endorsement notice

The text of ISO/IEC 27001:2013 including Cor 1:2014 and Cor 2:2015 has been approved by CEN as EN ISO/IEC 27001:2017 without any modification.

ÍST EN ISO/IEC 27001:2017

Efnisyfirlit

Contents

ÍST EN ISO/IEC 27001:2017

Formáli

ISO (International Organization for Standardization – Alþjóðlegu staðlasamtökin) og IEC (International Electrotechnical Commission – Alþjóða raftækniráðið) mynda sérhæft kerfi fyrir alþjóðlega stöðlun. Staðlastofnanir einstakra landa sem eiga aðild að ISO eða IEC taka þátt í þróun alþjóðastaðla með starfrækslu tækninefnda sem hvor staðlasamtökin um sig setja á fót til að fást við afmörkuð tæknisvið. Tækninefndir ISO og IEC hafa samvinnu um efnissvið sem hagsmunir þeirra beggja tengjast. Aðrar alþjóðlegar stofnanir, bæði þær sem starfa á vegum ríkisstjórna og aðrar, taka einnig þátt, í samvinnu við ISO og IEC. Á sviði upplýsingatækni hafa ISO og IEC komið á fót sameiginlegri tækninefnd, ISO/IEC JTC 1.

Alþjóðastaðlar eru samdir í samræmi við Vinnureglur ISO/IEC, 2. hluta.

Meginverkefni sameiginlegu tækninefndarinnar er að semja alþjóðastaðla. Frumvörp að alþjóðastöðlum, sem sameiginlega tækninefndin hefur komið sér saman um, eru send aðilum samtakanna til atkvæðagreiðslu. Alþjóðastaðall er ekki gefinn út nema að minnsta kosti 75 % þeirra aðila sem greiða atkvæði hafi samþykkt staðalinn.

Athygli er vakin á því að sum atriði í þessu skjali gætu fallið undir einkaleyfi. ISO og IEC bera ekki ábyrgð á að tilgreina einstök eða öll slík einkaleyfi.

Alþjóðastaðallinn ISO/IEC 27001 var saminn af sameiginlegu tækninefndinni ISO/IEC JTC 1, *Information technology*, undirnefnd SC 27, *IT Security techniques.*

Þessi önnur útgáfa fellir úr gildi og kemur í stað fyrstu útgáfu (ISO/IEC 27001:2005), sem hefur verið tæknilega endurskoðuð.

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

ISO/IEC 27001 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

This second edition cancels and replaces the first edition (ISO/IEC 27001:2005), which has been technically revised.

0 Inngangur

0.1 Almennt

Þessi alþjóðastaðall var saminn til þess að láta í té kröfur við að koma upp, innleiða, viðhalda og bæta stöðugt stjórnunarkerfi um upplýsingaöryggi. Það er stefnumarkandi ákvörðun fyrir skipulagsheild að taka upp stjórnunarkerfi um upplýsingaöryggi. Þarfir og markmið skipulagsheildarinnar, öryggiskröfur, þau skipulagsferli sem hún beitir, sem og stærð hennar og formgerð hefur áhrif á stofnun og innleiðingu stjórnunarkerfis um upplýsingaöryggi í skipulagsheildinni. Gert er ráð fyrir að allir þessir áhrifaþættir taki breytingum með tímanum.

Stjórnunarkerfið um upplýsingaöryggi varðveitir leynd, réttleika og tiltækileika upplýsinga með því að beita áhættustjórnunarferli og leiðir til trausts hagsmunaaðila á því að áhættu sé stjórnað með viðunandi hætti.

Mikilvægt er að stjórnunarkerfi um upplýsingaöryggi sé hluti af samþættum ferlum skipulagsheildarinnar og heildarskipulagi stjórnunar hennar og að litið sé til upplýsingaöryggis við hönnun ferla, upplýsingakerfa og stýringa. Gert er ráð fyrir því að við innleiðingu stjórnunarkerfis um upplýsingaöryggi verði umfang þess í samræmi við þarfir skipulagsheildarinnar.

Þennan alþjóðastaðal geta aðilar innan og utan skipulagsheildarinnar notað til þess að meta getu hennar til þess að uppfylla eigin kröfur um upplýsingaöryggi.

Röðin á kröfunum sem kynntar eru í þessum alþjóðastaðli endurspeglar hvorki mikilvægi þeirra né felur í sér í hvaða röð þær skuli innleiddar. Atriðin á listunum eru einvörðungu númeruð í tilvísunarskyni.

ÍST ISO/IEC 27000 lýsir yfirliti og orðaforða stjórnunarkerfa um upplýsingaöryggi með vísan til staðlaraðar fyrir stjórnunarkerfi um upplýsingaöryggi (þ.m.t. ISO/IEC 27003[2], ISO/IEC 27004[3] og ISO/IEC 27005[4]), ásamt tengdum hugtökum og skilgreiningum.

0.2 Samhæfi við staðla fyrir önnur stjórnunarkerfi

Í alþjóðastaðli þessum er beitt sömu heildaruppbyggingu, samhljóða fyrirsögnum undirgreina, samhljóða kjarnatexta, sameiginlegum hugtökum og kjarnaskilgreiningum sem skilgreindar eru í Viðauka SL við samantekna ISO viðbætinn við 1. hluta Vinnureglna ISO/IEC, og heldur hann því samhæfi við aðra stjórnunarkerfisstaðla sem gerðir eru í samræmi við viðauka SL.

Hin sameiginlega nálgun sem skilgreind er í viðauka SL mun gagnast þeim skipulagsheildum sem velja að starfrækja eitt stjórnunarkerfi sem uppfyllir kröfur tveggja eða fleiri stjórnunarkerfisstaðla.

0 Introduction

0.1 General

This International Standard has been prepared to provide requirements for establishing, implementing, maintaining and continually improving an information security management system. The adoption of an information security management system is a strategic decision for an organization. The establishment and implementation of an organization's information security management system is influenced by the organization's needs and objectives, security requirements, the organizational processes used and the size and structure of the organization. All of these influencing factors are expected to change over time.

The information security management system preserves the confidentiality, integrity and availability of information by applying a risk management process and gives confidence to interested parties that risks are adequately managed.

It is important that the information security management system is part of and integrated with the organization's processes and overall management structure and that information security is considered in the design of processes, information systems, and controls. It is expected that an information security management system implementation will be scaled in accordance with the needs of the organization.

This International Standard can be used by internal and external parties to assess the organization's ability to meet the organization's own information security requirements.

The order in which requirements are presented in this International Standard does not reflect their importance or imply the order in which they are to be implemented. The list items are enumerated for reference purpose only.

ISO/IEC 27000 describes the overview and the vocabulary of information security management systems, referencing the information security management system family of standards (including ISO/IEC 27003[2], ISO/IEC 27004[3] and ISO/IEC 27005[4]), with related terms and definitions.

0.2 Compatibility with other management system standards

This International Standard applies the high-level structure, identical sub-clause titles, identical text, common terms, and core definitions defined in Annex SL of ISO/IEC Directives, Part 1, Consolidated ISO Supplement, and therefore maintains compatibility with other management system standards that have adopted the Annex SL.

This common approach defined in the Annex SL will be useful for those organizations that choose to operate a single management system that meets the requirements of two or more management system standards.

Upplýsingatækni – Öryggisaðferðir – Stjórnunarkerfi um upplýsingaöryggi – Kröfur

1 Umfang

Í þessum alþjóðastaðli eru tilgreindar kröfur sem gilda um að koma á, innleiða, viðhalda og bæta stöðugt stjórnunarkerfi um upplýsingaöryggi í samhengi skipulagsheildarinnar. Þessi alþjóðastaðall felur einnig í sér kröfur varðandi mat og meðferð á upplýsingaöryggisáhættu sem sniðnar eru að þörfum skipulagsheildarinnar. Þær kröfur sem settar eru fram í þessum alþjóðastaðli eru almennar og er ætlunin að þeim megi beita á allar skipulagsheildir, óháð tegund, stærð og eðli. Óásættanlegt er að sleppa einhverjum af þeim kröfum sem tilgreindar eru í greinum 4 til 10 þegar skipulagsheild lýsir yfir samræmi við þennan alþjóðastaðal.

2 Tilvísanir í staðla

Eftirfarandi skjöl sem vísað er til, í heild eða að hluta, í þessu skjali, eru ómissandi við notkun þess. Dagsettar tilvísanir eiga aðeins við þá útgáfu sem vísað er í. Ódagsettar tilvísanir vísa til nýjustu útgáfu viðkomandi skjals (ásamt öllum breytingum).
ÍST EN ISO/IEC 27000, Upplýsingatækni – Öryggisaðferðir – Stjórnunarkerfi um upplýsingaöryggi – Yfirlit og orðaforði

3 Hugtök og skilgreiningar

Í þessu skjali gilda hugtök og skilgreiningar í ÍST EN ISO/IEC 27000.

4 Samhengi skipulagsheildar

4.1 Að skilja skipulagsheildina og samhengi hennar

Skipulagsheildin skal ákvarða ytri og innri málefni sem varða tilgang hennar og sem hafa áhrif á getu hennar til þess að ná þeirri útkomu eða útkomum sem stefnt er að með stjórnunarkerfi hennar um upplýsingaöryggi.

ATHUGASEMD Með ákvörðun þessara málefna er átt við mörkun ytra og innra samhengis skipulagsheildarinnar, sbr. grein 5.3 í ISO 31000:2009[5].

4.2 Að skilja þarfir og væntingar hagsmunaaðila

Skipulagsheildin skal ákvarða:
a) þá hagsmunaaðila sem skipta máli fyrir stjórnunarkerfið um upplýsingaöryggi; og
b) þær kröfur þessara hagsmunaaðila sem skipta máli fyrir upplýsingaöryggi.

ATHUGASEMD Kröfur hagsmunaaðila geta innihaldið kröfur laga og stjórnvaldsreglna og samningsbundnar skyldur.

4.3 Að ákvarða umfang stjórnunarkerfisins um upplýsingaöryggi

Skipulagsheildin skal ákvarða mörk og notkunarsvið stjórnunarkerfisins um upplýsingaöryggi til þess að ákveða umfang þess.

Þegar þetta umfang er ákvarðað skal skipulagsheildin íhuga:
a) ytri og innri málefni sem vísað er til í 4.1;
b) kröfurnar sem vísað er til í 4.2; og
c) skilfleti og vensl milli athafna skipulagsheildarinnar og athafna annarra skipulagsheilda.

Umfangið skal vera tiltækt sem skjalfestar upplýsingar.