Avaldatud eesti keeles: märts 2017
Jõustunud Eesti standardina: märts 2017

INFOTEHNOLOOGIA
Turbemeetodid
Infoturbe halduse süsteemid
Nõuded

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

EESTI STANDARDIKESKUS
ESTONIAN CENTRE FOR STANDARDISATION

EESTI STANDARDI EESSÕNA

See Eesti standard on

— Euroopa standardi EN ISO/IEC 27001:2017 ingliskeelse teksti sisu poolest identne tõlge eesti keelde. Tõlgenduserimeelsuste korral tuleb lähtuda ametlikes keeltes avaldatud tekstidest;

— jõustunud Eesti standardina inglise keeles märtsis 2017;

— eesti keeles avaldatud sellekohase teate ilmumisega EVS Teataja 2017. aasta märtsikuu numbris.

Standardi tõlke koostamise ettepaneku on esitanud tehniline komitee EVS/TK 4 „Infotehnoloogia“, standardi tõlkimist on korraldanud Eesti Standardikeskus ning rahastanud Majandus- ja Kommunikatsiooniministeerium.

Standardi on tõlkinud Cybernetica AS, standardi on heaks kiitnud EVS/TK 4.

See standard EVS-EN ISO/IEC 27001:2017, mille alusdokumendiks on muutmata kujul Euroopa standardina üle võetud rahvusvaheline standard ISO/IEC 27001:2013, on sisult identne 2014. a oktoobris jõustunud Eesti standardiga EVS-ISO/IEC 27001:2014.

Euroopa standardimisorganisatsioonid on teinud Euroopa standardi EN ISO/IEC 27001:2017 rahvuslikele liikmetele kättesaadavaks 22.02.2017.

Date of Availability of the European Standard EN ISO/IEC 27001:2017 is 22.02.2017.

See standard on Euroopa standardi EN ISO/IEC 27001:2017 eestikeelne [et] versioon. Teksti tõlke on avaldanud Eesti Standardikeskus ja sellel on sama staatus ametlike keelte versioonidega.

This standard is the Estonian [et] version of the European Standard EN ISO/IEC 27001:2017. It was translated by the Estonian Centre for Standardisation. It has the same status as the official versions.

Tagasisidet standardi sisu kohta on võimalik edastada, kasutades EVS-i veebilehel asuvat tagasiside vormi või saates e-kirja meiliaadressile standardiosakond@evs.ee.

ICS 35.040

EUROOPA STANDARD
EUROPEAN STANDARD
NORME EUROPÉENNE
EUROPÄISCHE NORM

EN ISO/IEC 27001

February 2017

ICS 03.100.70; 35.030

English Version

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)

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

This European Standard was approved by CEN on 26 January 2017.

CEN and CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration. Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CEN and CENELEC member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CEN and CENELEC member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CEN and CENELEC members are the national standards bodies of 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 United Kingdom.

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

CEN-CENELEC Management Centre: Avenue Marnix 17, B-1000 Brussels

Ref. No. EN ISO/IEC 27001:2017 E

SISUKORD

EUROOPA EESSÕNA

Dokumendi (ISO/IEC 27001:2013, sealhulgas Cor 1:2014 ja Cor 2:2015) on koostanud Rahvusvahelise Standardimisorganisatsiooni (*International Organization for Standardization*, ISO) ja Rahvusvahelise Elektrotehnikakomisjoni (*International Electrotechnical Commission*, IEC) tehniline komitee ISO/IEC JTC 1 „Information technology“ ning see on üle võetud standardina EN ISO/IEC 27001:2017.

Euroopa standardile tuleb anda rahvusliku standardi staatus kas identse tõlke avaldamisega või jõustumisteatega hiljemalt 2017. a augustiks ja sellega vastuolus olevad rahvuslikud standardid peavad olema kehtetuks tunnistatud hiljemalt 2017. a augustiks.

Tuleb pöörata tähelepanu võimalusele, et standardi mõni osa võib olla patendiõiguse objekt. CEN [ja/või CENELEC] ei vastuta sellis(t)e patendiõigus(t)e väljaselgitamise ega selgumise eest.

CEN-i/CENELEC-i sisereeglite järgi peavad Euroopa standardi kasutusele võtma järgmiste riikide rahvuslikud standardimisorganisatsioonid: Austria, Belgia, Bulgaaria, Eesti, endine Jugoslaavia Makedoonia Vabariik, Iirimaa, Island, Itaalia, Hispaania, Holland, Horvaatia, Kreeka, Küpros, Leedu, Luksemburg, Läti, Malta, Norra, Poola, Portugal, Prantsusmaa, Rootsi, Rumeenia, Saksamaa, Serbia, Slovakkia, Sloveenia, Soome, Šveits, Taani, Tšehhi Vabariik, Türgi, Ungari ja Ühendkuningriik.

Jõustumisteade

CEN on standardi ISO/IEC 27001:2013, sealhulgas Cor 1:2014 ja Cor 2:2015 teksti muutmata kujul üle võtnud standardina EN ISO/IEC 27001:2017.

0 SISSEJUHATUS

0.1 Üldist

See standard on koostatud eesmärgiga anda nõuded infoturbe halduse süsteemi rajamiseks, evituseks, käigushoiuks ja pidevaks täiustamiseks. Infoturbe halduse süsteemi kasutuselevõtt on üks organisatsiooni strateegilisi otsuseid. Organisatsiooni infoturbe halduse süsteemi rajamist ja evitust mõjutavad organisatsiooni vajadused ja eesmärgid, turvanõuded, kasutatavad protsessid ning organisatsiooni suurus ja struktuur. Eeldatavalt muutuvad kõik need mõjurid ajas.

Riskihalduse protsessi rakendades säilitab see infoturbe halduse süsteem teabe konfidentsiaalsuse, tervikluse ja käideldavuse ning annab huvipooltele kindlustunde riskide adekvaatse valitsemise suhtes.

On tähtis, et infoturbe halduse süsteem oleks organisatsiooni protsesside ja üldise haldusstruktuuri lahutamatu osa ning et infoturvet arvestataks protsesside, infosüsteemide ja juhtimismeetmete kavandamisel. Eeldatavalt muudetakse infoturbe halduse süsteemi teostuse mastaapi vastavalt organisatsiooni vajadustele.

Seda standardit saavad sisemised ja välised pooled kasutada organisatsiooni võimekuse hindamiseks omaenda infoturvanõuete täitmisel.

Nõuete esituse järjestus selles standardis ei kajasta nende tähtsust ega tähenda nende rakendamise järjestust. Loetelupunktid on nummerdatud ainult neile viitamiseks.

ISO/IEC 27000 esitab infoturbe halduse süsteemide ülevaate ja sõnavara, viidates infoturbe halduse süsteemi standardiperele (millesse kuuluvad ISO/IEC 27003[2], ISO/IEC 27004[3] ja ISO/IEC 27005[4]), koos seotud terminite ja määratlustega.

0.2 Ühilduvus muude haldussüsteemide standarditega

See standard kohaldab sellist üldstruktuuri, selliseid alajaotiste pealkirju, sellist teksti, selliseid üldisi termineid ja keskseid määratlusi, mis on määratletud ISO/IEC direktiivide 1. osa (ISO konsolideeritud täiendosa) lisas SL, säilitades seega ühilduvuse muude haldussüsteemide standarditega, mis on kohaldanud lisa SL.

See lisas SL määratletud ühine käsitlusviis on kasulik neile organisatsioonidele, kes eelistavad hoida käigus ühtainsat haldussüsteemi, mis vastab mitme haldussüsteemi standarditele.

1 KÄSITLUSALA

See standard spetsifitseerib nõuded infoturbe halduse süsteemi rajamiseks, evituseks, käigushoiuks ja pidevaks täiustamiseks organisatsiooni kontekstis. Standard sisaldab ka nõudeid organisatsiooni vajadustele kohandatavaks infoturvariskide kaalutlemiseks ja käsitluseks. Selles standardis püstitatud nõuded on üldistuslikud ning on mõeldud kohaldatavaks kõigile organisatsioonidele, sõltumata nende tüübist, suurusest või iseloomust. Kui organisatsioon taotleb vastavust sellele standardile, ei tohi ta välistada ühtki peatükkides 4 kuni 10 spetsifitseeritud nõuet.

2 NORMIVIITED

Alljärgnevalt nimetatud dokumendid, mille kohta on standardis esitatud normiviited, on kas tervenisti või osaliselt vajalikud selle standardi rakendamiseks. Dateeritud viidete korral kehtib üksnes viidatud väljaanne. Dateerimata viidete korral kehtib viidatud dokumendi uusim väljaanne koos võimalike muudatustega.

ISO/IEC 27000. Information technology — Security techniques — Information security management systems — Overview and vocabulary

3 TERMINID JA MÄÄRATLUSED

Standardi rakendamisel kasutatakse standardis ISO/IEC 27000 esitatud termineid ja määratlusi.

4 ORGANISATSIOONI KONTEKST

4.1 Organisatsiooni ja ta konteksti tundmaõppimine

Organisatsioon peab kindlaks tegema sisemised ja välised probleemid, mis puudutavad ta eesmärki ning mõjutavad ta võimet saavutada oma infoturbe halduse süsteemilt oodatavaid tulemusi.

MÄRKUS Nende probleemide kindlakstegemine toetub organisatsiooni sisemise ja välise konteksti väljaselgitamisele, mida käsitleb ISO 31000:2009[5] jaotis 5.3.

4.2 Huvipoolte vajaduste ja ootuste tundmaõppimine

Organisatsioon peab välja selgitama

a) infoturbe halduse süsteemi jaoks asjakohased huvipooled;

b) nende huvipoolte nõuded, mis on infoturbe suhtes asjakohased.

MÄRKUS Huvipoolte nõuete hulka võivad kuuluda õigusaktide ja eeskirjade nõuded ning lepingulised kohustused.

4.3 Infoturbe halduse süsteemi käsitlusala määramine

Infoturbe halduse süsteemi käsitlusala kehtestamiseks peab organisatsioon määrama selle süsteemi piirid ja kohaldatavuse.

Selle käsitlusala määramisel peab organisatsioon võtma arvesse

a) jaotises 4.1 mainitud sisemisi ja väliseid probleeme;

b) jaotises 4.2 nimetatud nõudeid;

c) organisatsiooni sooritatavate tegevuste ja teiste organisatsioonide sooritatavate tegevuste vahelisi liideseid ja sõltuvusi.