Avaldatud eesti keeles: oktoober 2014
Jõustunud Eesti standardina: oktoober 2014

INFOTEHNOLOOGIA
Turbemeetodid
Infoturbe halduse süsteemid
Nõuded

Information technology
Security techniques
Information security management systems
Requirements
(ISO/IEC 27001:2013 + Cor 1:2014)

EESTI STANDARDIKESKUS
ESTONIAN CENTRE FOR STANDARDISATION

EESTI STANDARDI EESSÕNA

See Eesti standard on

— rahvusvahelise standardi ISO/IEC 27001:2013 ning selle paranduste Cor 1:2014 ja Cor 2:2015 inglis-keelsete tekstide sisu poolest identne konsolideeritud tõlge eesti keelde. Tõlgenduserimeelsuste korral tuleb lähtuda ametlikes keeltes avaldatud tekstidest;

— jõustunud Eesti standardina sellekohase teate avaldamisega EVS Teataja 2014. aasta oktoobrikuu numbris.

Standardi on tõlkinud Cybernetica AS, standardi tõlke on heaks kiitnud EVS/TK 4 „Infotehnoloogia“.

Standardi tõlkimise ettepaneku on esitanud EVS/TK 4, standardi tõlkimist on korraldanud Eesti Standardikeskus ning rahastanud Majandus- ja Kommunikatsiooniministeerium.

Sellesse standardisse on parandused ISO/IEC 27001:2013/Cor 1:2014 ja EVS-ISO/IEC 27001:2014/AC:2015 sisse viidud ja tehtud parandused tähistatud vastavalt püstkriipsu ja siksakjoonega lehe välisveerisel.

See standard on rahvusvahelise standardi ISO/IEC 27001:2013 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 International Standard ISO/IEC 27001:2013. It has been 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 Märgistikud ja informatsiooni kodeerimine

SISUKORD

EESSÕNA

ISO (Rahvusvaheline Standardimisorganisatsioon) ja IEC (Rahvusvaheline Elektrotehnikakomisjon) moodustavad ülemaailmse standardimise spetsialiseeritud süsteemi. ISO või IEC rahvuslikud liikmesorganisatsioonid osalevad rahvusvaheliste standardite väljatöötamises tehniliste komiteede kaudu, mis on nendes organisatsioonides rajatud käsitlema tehnilise tegevuse eri valdkondi. ISO ja IEC tehnilised komiteed teevad koostööd mõlemale huvi pakkuvatel aladel. Selles töös osalevad käsikäes ISO ja IEC-ga ka rahvusvahelised, riiklikud ja valitsusvälised organisatsioonid. Infotehnoloogia valdkonnas on ISO ja IEC rajanud ühendatud tehnilise komitee ISO/IEC JTC 1.

Rahvusvahelised standardid kavandatakse ISO/IEC direktiivide 2. osas esitatud reeglite kohaselt.

Ühendatud tehnilise komitee põhiülesanne on rahvusvaheliste standardite koostamine. Ühendatud tehnilises komitees vastuvõetud rahvusvahelised standardikavandid saadetakse hääletamiseks liikmesorganisatsioonidele. Avaldamine rahvusvahelise standardina nõuab, et hääletanud liikmesorganisatsioonidest kiidaks selle heaks vähemalt 75 %.

Tuleb pöörata tähelepanu võimalusele, et standardi mõni osa võib olla patendiõiguse subjekt. ISO-t ega IEC-d ei saa pidada vastutavaks sellis(t)e patendiõigus(t)e väljaselgitamise eest.

Standardi ISO/IEC 27001 on koostanud ühendatud tehnilise komitee ISO/IEC JTC 1 „Infotehnoloogia“ alamkomitee SC 27 „Infoturbemeetodid“.

See, teine redaktsioon tühistab ja asendab esimest redaktsiooni (ISO/IEC 27001:2005), olles selle tehniline uustöötlus.

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 oma-enda 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.

Taotluslikult tühjaks jäetud

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.

Käsitlusala peab olemas olema dokumenteeritud teabena.