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

INFOTEHNOLOOGIA
Turbemeetodid
Infoturbemeetodite tavakoodeks

Information technology
Security techniques
Code of practice for information security controls (ISO/IEC 27002:2013 including Cor 1:2014 and Cor 2:2015)

EESTI STANDARDI EESSÕNA

See Eesti standard on

— Euroopa standardi EN ISO/IEC 27002:2017 ingliskeelse teksti sisu poolest identne tõlge eesti keelde ja sellel on sama staatus mis jõustumisteate meetodil vastuvõetud originaalversioonil. 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 AS Cybernetica, standardi on heaks kiitnud EVS/TK 4.

See standard EVS-EN ISO/IEC 27002:2017, mille alusdokumendiks on muutmata kujul Euroopa standardina üle võetud rahvusvaheline standard ISO/IEC 27002:2013, on sisult identne 2014. a oktoobris jõustunud Eesti standardiga EVS-ISO/IEC 27002:2014.

Euroopa standardimisorganisatsioonid on teinud Euroopa standardi EN ISO/IEC 27002:2017 rahvuslikele liikmetele kättesaadavaks 22.02.2017.

Date of Availability of the European Standard EN ISO/IEC 27002:2017 is 22.02.2017.

See standard on Euroopa standardi EN ISO/IEC 27002:2017 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 27002:2017. 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 03.100.70; 35.030

EESTI STANDARD
EUROPEAN STANDARD
NORME EUROPÉENNE
EUROPÄISCHE NORM

EN ISO/IEC 27002

February 2017

ICS 03.100.70; 35.030

English Version

Information technology - Security techniques - Code of practice for information security controls (ISO/IEC 27002:2013 including Cor 1:2014 and Cor 2:2015)

Technologies de l'information - Techniques de sécurité - Code de bonne pratique pour le management de la sécurité de l'information (ISO/IEC 27002:2013 y compris Cor 1:2014 et Cor 2:2015)

Informationstechnik - Sicherheitsverfahren - Leitfaden für Informationssicherheitsmaßnahmen (ISO/IEC 27002:2013 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 27002:2017 E

SISUKORD

EUROOPA EESSÕNA

Dokumendi (ISO/IEC 27002:2013, 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 27002:2017.

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, Hispaania, Holland, Horvaatia, Iirimaa, Island, Itaalia, 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 27002:2013, sealhulgas paranduste Cor 1:2014 ja Cor 2:2015 teksti muutmata kujul üle võtnud standardina EN ISO/IEC 27002:2017.

0 SISSEJUHATUS

0.1 Taustateave ja kontekst

See standard on kavandatud organisatsioonidele teatmikuna meetmete valimiseks standardil ISO/IEC 27001[10] põhineva infoturbe halduse süsteemi (Information Security Management System, ISMS) evitamise protsessi raames, või suunisena organisatsioonidele, kes evitavad üldtunnustatud infoturvameetmeid. Standard on ühtlasi mõeldud kasutamiseks tööstusele ja organisatsioonile spetsiifiliste infoturbehalduse suuniste välja töötamiseks, arvestades nende konkreetset infoturvariski keskkonda või -keskkondi.

Igat tüüpi ja suurusega organisatsioonid (sealhulgas avaliku ja erasektori, äri- ja mittetulundusorganisatsioonid) koguvad, töötlevad, talletavad ja edastavad teavet mitmel kujul, sealhulgas elektroonilisel, füüsilisel ja sõnalisel (nt vestlused ja esitlused).

Teabe väärtus ulatub kaugemale kirjapandud sõnadest, arvudest ja piltidest – teadmus, mõisted, ideed ja kaubamärgid on näited immateriaalsetest teabevormidest. Ühenduses olevas maailmas on teave ja temaga seotud protsessid, süsteemid, võrgud ja nende käituses osalevad inimesed varadeks, mis, nagu muudki tähtsad talitlusvarad, on organisatsiooni tegevusele väärtuslikud ja seega väärivad või nõuavad asjakohast kaitset mitmesuguste ohtude eest.

Varad on nii sihilike kui ka ettekavatsemata ohtude objektiks, samas kui asjassepuutuvail protsessidel, süsteemidel, võrkudel ja inimestel on loomuomased nõrkused. Muudatused talitlusprotsessides ja süsteemides või teised välised muudatused (näiteks uued õigusaktid ja eeskirjad) võivad luua uusi infoturvariske. Arvestades rohkeid viise, kuidas ohud saavad nõrkusi organisatsiooni kahjustamiseks ära kasutada, jäävad infoturvariskid seetõttu alati alles. Tõhus infoturve vähendab riske, kaitstes organisatsiooni ohtude ja nõrkuste eest ning vähendades siis mõjusid ta varadele.

Teabe turvalisus saavutatakse, rakendades sobivat meetmestikku, sealhulgas poliitikaid, protsesse, protseduure, organisatsioonilisi struktuure ning tarkvara- ja riistvarafunktsioone. Organisatsiooni konkreetsete turva- ja tegevuseesmärkide saavutamise tagamiseks tuleb neid meetmeid kehtestada, evitada, seirata, läbi vaadata ja vajaduse korral täiustada. Selline ISMS, nagu määratleb ISO/IEC 27001[10], vaatleb organisatsiooni infoturvariske terviklikult ja koordineeritult, et evitada laiaulatuslik infoturvameetmete komplekt sidusa haldussüsteemi üldises raamistikus.

Paljud infosüsteemid pole kavandatud turvalisteks ISO/IEC 27001[10] ja selle standardi tähenduses. Tehniliste vahenditega võib saavutada piiratud turvet ning seda tuleks toetada sobiva halduse ja protseduuridega. Vajalike meetmete väljaselgitamine nõuab hoolikat plaanimist ja üksikasjadele tähelepanu pööramist. Edukas ISMS vajab organisatsiooni kõigi töötajate toetust. See võib nõuda ka aktsionäride, tarnijate või muude väliste poolte osalust. Vajalikuks võivad osutuda ka väliste poolte asjatundjate nõuanded.

Üldisemas tähenduses annab toimiv infoturve ühtlasi juhtkonnale ja teistele huvipooltele kinnituse, et organisatsiooni varad on mõistlikult turvatud ja kahjude eest kaitstud, toimides seega talitluse võimaldajana.

0.2 Nõuded teabe turvalisusele

On oluline, et organisatsioon selgitaks välja oma turvanõuded. Selleks on kolm peamist allikat:

a) organisatsiooni riskide kaalutlemine, mis arvestab organisatsiooni üldist tegutsemise strateegiat ja eesmärke. Riskide kaalutlemise teel tuvastatakse ohud varadele, hinnatakse nõrkuseid ohtude suhtes ja ohtude teostumise tõenäosust ning hinnatakse nende võimalikku toimet;

b) õigusaktide, statuudi, eeskirjade ja lepingute nõuded, mida peavad täitma organisatsioon, ta äripartnerid, töövõtjad ja teenuseandjad, ning nende sotsiaalne ja kultuuriline keskkond;

c) teabe käitlemise, töötlemise, talletamise, edastamise ja arhiveerimise printsiipide, eesmärkide ja talitlusnõuete kogum, mille organisatsioon on välja töötanud oma tegevuse toeks.

Meetmete evitamiseks kasutatavad ressursid tuleb tasakaalustada äriliste kahjudega, mis võivad nende meetmete puudumisel turvariketest tuleneda. Riski kaalutlemise tulemused aitavad suunata ja määrata sobivaid haldustoiminguid ja prioriteete teabe infoturvariskide halduseks ja nende riskide eest kaitsma valitud turvameetmete rakendamiseks.

Standard ISO/IEC 27005[11] annab suunised infoturvariskide halduseks, sealhulgas nõuandeid riskide kaalutlemiseks, käsitlemiseks, aktsepteerimiseks, teavituseks, seireks ja läbivaatuseks.

0.3 Turvameetmete valimine

Sõltuvalt olukorrast võib turvameetmeid valida sellest standardist või muudest meetmestikest või töötada erivajaduste rahuldamiseks välja uusi.

Meetmete valimine sõltub organisatsiooni otsustest, mis põhinevad riski aktsepteerimise kriteeriumidel, riski käsitluse võimalustel ja üldisest organisatsioonis rakendatavast riskihalduse metoodikast, ning peaksid järgima ka kõiki asjassepuutuvaid riiklikke ja rahvusvahelisi õigusakte ja eeskirju. Turvameetmete valimine sõltub ka meetmete koostoimeviisist, et tagada sügavuti kaitse.

Mõningaid selles standardis leiduvaid turvameetmeid võib lugeda infoturbe haldust suunavateks põhimõteteks ja nad on kohaldatavad enamikule organisatsioonidele. Neid on selgitatud üksikasjalikumalt allpool koos nende rakendusjuhistega. Lisateavet meetmete valimise ja muude riski käsitlemise võimaluste kohta on standardis ISO/IEC 27005[11].

0.4 Omaenda suuniste väljatöötamine

Seda standardit võib lugeda lähtepunktiks, millest alustada organisatsioonispetsiifiliste suuniste väljatöötamist. Kõik selles tavakoodeksis leiduvad suunised ja meetmed ei ole võib-olla rakendatavad. Peale selle võivad osutuda vajalikeks lisameetmed, mida see standard ei sisalda. Kui koostatakse dokumente, mis sisaldavad lisasuuniseid või -meetmeid, on ehk kasulik kohaldatavail juhtudel lisada viited selle standardi jaotistele, et hõlbustada audiitoritel ja äripartneritel vastavuse kontrollimist.

0.5 Elutsükli kaalutlusi

Teabel on loomulik elutsükkel loomisest ja algatamisest läbi talletuse, töötluse, kasutuse ja edastuse kuni tema lõpliku hävitamise või riknemiseni. Varade väärtus ja risk neile võib nende eluaja jooksul muutuda (näiteks ettevõtte rahastamiskontode volitamata paljastamine või vargus on märksa vähem oluline pärast nende formaalset avaldamist), kuid teabe turvalisus jääb teatud määrani oluliseks kõigis järkudes.

Infosüsteemidel on elutsüklid, mille piires nad luuakse, spetsifitseeritakse, kavandatakse, töötatakse välja, testitakse, evitatakse, neid kasutatakse, hooldatakse, ja lõpuks kasutusest eemaldatakse ja kõrvaldatakse. Infoturvet tuleks arvesse võtta igas järgus. Uued süsteemiarendused ja seniste süsteemide muudatused pakuvad organisatsioonidele võimalusi turvameetmete värskendamiseks ja parandamiseks, võttes arvesse tegelikke intsidente ning praegusi ja prognoositavaid infoturvariske.

0.6 Sidusstandardid

Ehkki see standard annab suuniseid mitmesuguste infoturvameetmete kohta, mida sageli rakendatakse paljudes erinevates organisatsioonides, annavad ülejäänud ISO/IEC 27000 perekonna standardid lisanõuandeid või -nõudeid teiste aspektide kohta üldises infoturbehalduse protsessis.

Pöörduge ISO/IEC 27000 poole üldiseks sissejuhatuseks nii ISMSide kui ka selle standardiperekonna kohta. ISO/IEC 27000 annab sõnastiku, mis määratleb formaalselt enamiku ISO/IEC 27000 standardiperekonnas läbivalt kasutatavatest termineist ning kirjeldab iga standardipere liikme käsitlusala ja eesmärki.

1 KÄSITLUSALA

See rahvusvaheline standard annab suunised organisatsiooni infoturbestandardite ja infoturbehalduse praktikate kohta, sealhulgas kuidas valida, rakendada ja hallata meetmeid, võttes arvesse organisatsiooni infoturberiski keskkonda või -keskkondi.

See rahvusvaheline standard on kavandatud kasutamiseks organisatsioonides, kes kavatsevad

a) valida meetmeid protsessi käigus, millega teostatakse standardil ISO/IEC 27001 põhinev infoturbehalduse süsteem [10];

b) teostada üldtunnustatud infoturbemeetmed;

c) välja arendada omaenda infoturbehalduse suunised.

2 NORMIVIITED

Alljärgnevalt nimetatud dokumendid, mille kohta on standardis esitatud normviited, 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 SELLE STANDARDI STRUKTUUR

Standard sisaldab 14 turvameetmete peatükki, mis kokku sisaldavad 35 põhilist turvakategooriat ja 114 turvameedet.

4.1 Peatükid

Iga peatükk, mis määratleb turvameetme, sisaldab ühte või mitut peamist turvakategooriat.

Peatükkide järjestus standardis ei määra nende olulisust. Sõltuvalt asjaoludest võivad olulised olla turvameetmed ükskõik millisest peatükist või kõigist peatükkidest, mistõttu iga organisatsioon, kes rakendab seda standardit, peaks kindlaks tegema kohaldatavad meetmed, nende olulisuse ja rakendatavuse igale äriprotsessile. Lisaks pole standardi loetelud tähtsuse järjekorras.

4.2 Meetmeliigid

Iga peamine turvameetme liik sisaldab

a) juhtimiseesmärki, mis sõnastab selle, mis tuleb saavutada; ja

b) üht või mitut turvameedet, mida tuleb rakendada selle juhtimiseesmärgi saavutamiseks.

Meetmete kirjeldused on struktureeritud alljärgnevalt:

Meede

Määratleb konkreetse juhtimissätte, millega saavutada juhtimiseesmärk.