Avaldatud eesti keeles: märts 2024
Jõustunud Eesti standardina: august 2023

INFOTURVE, KÜBERTURVE JA PRIVAATSUSKAITSE
Infoturbe halduse süsteemid
Nõuded

Information security, cybersecurity and privacy protection
Information security management systems
Requirements
(ISO/IEC 27001:2022)

EVS • EESTI STANDARDIMIS- JA AKREDITEERIMISKESKUS
ESTONIAN CENTRE FOR STANDARDISATION AND ACCREDITATION

EESTI STANDARDI EESSÕNA

See Eesti standard on

— Euroopa standardi EN ISO/IEC 27001:2023 ingliskeelse teksti sisu poolest identne tõlge eesti keelde ja sellel on sama staatus mis jõustumisteate meetodil vastu võetud originaalversioonil. Tõlgenduserimeelsuste korral tuleb lähtuda ametlikes keeltes avaldatud tekstidest;

— jõustunud Eesti standardina inglise keeles augustis 2023;

— eesti keeles avaldatud sellekohase teate ilmumisega EVS Teataja 2024. aasta märtsikuu numbris.

Standardi tõlke koostamise ettepaneku on esitanud tehniline komitee EVS/TK 04 „Infotehnoloogia“, standardi tõlkimist on korraldanud Eesti Standardimis- ja Akrediteerimiskeskus ning rahastanud Majandus- ja Kommunikatsiooniministeerium.

Standardi on tõlkinud Cybernetica AS, standardi on heaks kiitnud EVS/TK 04.

Euroopa standardimisorganisatsioonid on teinud Euroopa standardi EN ISO/IEC 27001:2023 rahvusliikele liikmetele kättesaadavaks 26.07.2023.

Date of Availability of the European Standard EN ISO/IEC 27001:2023 is 26.07.2023.

See standard on Euroopa standardi EN ISO/IEC 27001:2023 eestikeelne [et] versioon. Teksti tõlke on avaldanud Eesti Standardimis- ja Akrediteerimiskeskus ning sellel on sama staatus ametlike keelte versioonidega.

This standard is the Estonian [et] version of the European Standard EN ISO/IEC 27001:2023. It was translated by the Estonian Centre for Standardisation and Accreditation. 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

EUROOPA STANDARD
EUROPEAN STANDARD
NORME EUROPÉENNE
EUROPÄISCHE NORM

EN ISO/IEC 27001

July 2023

ICS 03.100.70; 35.030

Supersedes EN ISO/IEC 27001:2017

English Version

Information security, cybersecurity and privacy protection — Information security management systems — Requirements (ISO/IEC 27001:2022)

Sécurité de l'information, cybersécurité et protection de la vie privée - Systèmes de management de la sécurité de l'information - Exigences (ISO/IEC 27001:2022)

Informationssicherheit, Cybersicherheit und Datenschutz - Informationssicherheitsmanagementsysteme - Anforderungen (ISO/IEC 27001:2022)

This European Standard was approved by CEN on 23 July 2023.

CEN 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, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Türkiye and United Kingdom.

CEN-CENELEC Management Centre:
Rue de la Science 23, B-1040 Brussels

Ref. No. EN ISO/IEC 27001:2023 E

SISUKORD

EUROOPA EESSÕNA 4
EESSÕNA 5
SISSEJUHATUS 6
1 KÄSITLUSALA 7
2 NORMIVIITED 7
3 TERMINID JA MÄÄRATLUSED 7
4 ORGANISATSIOONI KONTEKST 7
4.1 Organisatsiooni ja ta konteksti tundmaõppimine 7
4.2 Huvipoolte vajaduste ja ootuste tundmaõppimine 7
4.3 Infoturbe halduse süsteemi käsitlusala määramine 7
4.4 Infoturbe halduse süsteem 8
5 EESTVEDU 8
5.1 Eestvedu ja kohustumus 8
5.2 Poliitika 8
5.3 Organisatsioonilised rollid, kohustused ja õigused 9
6 KAVANDAMINE 9
6.1 Toimingud riskide ja soodsate võimaluste arvestamiseks 9
6.1.1 Üldist 9
6.1.2 Infoturvariski kontroll 9
6.1.3 Infoturvariski käsitlemine 10
6.2 Infoturvaeesmärgid ja kavandamine nende saavutamiseks 10
6.3 Muudatuste kavandamine 11
7 TUGI 11
7.1 Ressursid 11
7.2 Pädevus 11
7.3 Teadlikkus 11
7.4 Teavitus 12
7.5 Dokumenteeritud teave 12
7.5.1 Üldist 12
7.5.2 Loomine ja ajakohastamine 12
7.5.3 Dokumenteeritud teabe ohje 12
8 KÄITUS 13
8.1 Käituse kavandamine ja juhtimine 13
8.2 Infoturvariski kaalutlemine 13
8.3 Infoturvariski käsitlemine 13
9 SOORITUSE HINDAMINE 13
9.1 Seire, mõõtmine, analüüs ja hindamine 13
9.2 Siseaudit 14
9.2.1 Üldist 14
9.2.2 Siseauditi tegevuskava 14
9.3 Juhtkondlik läbivaatus 14
9.3.1 Üldist 14
9.3.2 Juhtkondliku läbivaatuse lähteandmed 14
9.3.3 Juhtkondliku läbivaatuse tulemid 15
10 TÄIUSTAMINE 15
10.1 Pidev täiustamine 15

10.2 Lahknevus ja parandusmeetmed 15
Lisa A (normlisa) Infoturvameetmete viited 16
Kirjandus 25

EUROOPA EESSÕNA

ISO/IEC 27001:2022 teksti on koostanud Rahvusvahelise Standardimisorganisatsiooni (ISO) tehniline komitee ISO/IEC JTC 1 „Information technology“ ja selle on standardina EN ISO/IEC 27001:2023 üle võtnud tehniline komitee CEN-CENELEC/ JTC 13 „Cybersecurity and Data Protection“, mille sekretariaati haldab DIN.

Euroopa standardile tuleb anda rahvusliku standardi staatus kas identse tõlke avaldamisega või jõustumisteatega hiljemalt 2024. a jaanuariks ja sellega vastuolus olevad rahvuslikud standardid peavad olema kehtetuks tunnistatud hiljemalt 2024. a jaanuariks.

Tuleb pöörata tähelepanu võimalusele, et dokumendi mõni osa võib olla patendiõiguse objekt. CEN-CENELEC ei vastuta sellis(t)e patendiõigus(t)e väljaselgitamise ega selgumise eest.

See dokument asendab standardit ISO/IEC 27001:2017.

Igasugune tagasiside ja küsimused selle dokumendi kohta tuleks suunata dokumendi kasutaja rahvuslikule standardimisorganisatsioonile. Täielik loetelu nende organisatsioonide kohta on leitav CEN-i ja CENELEC-i veebilehtedelt.

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

Jõustumisteade

CEN-CENELEC on dokumendi ISO/IEC 27001:2022 teksti muutmata kujul üle võtnud kui EN ISO/IEC 27001:2023.

EESSÕNA

ISO (International Organization for Standardization) on ülemaailmne rahvuslike standardimisorganisatsioonide (ISO rahvuslike liikmesorganisatsioonide) föderatsioon. Tavaliselt tegelevad rahvusvahelise standardi koostamisega ISO tehnilised komiteed. Kõigil rahvuslikel liikmesorganisatsioonidel, kes on mingi tehnilise komitee pädevusse kuuluvast valdkonnast huvitatud, on õigus selle komitee tegevusest osa võtta. Selles töös osalevad ka ISO-ga seotud rahvusvahelised riiklikud organisatsioonid ning vabaühendused. Kõigis elektrotehnika standardimist puudutavates küsimustes teeb ISO tihedat koostööd Rahvusvahelise Elektrotehnikakomisjoniga (IEC).

Selle dokumendi väljatöötamiseks kasutatud ja edasiseks haldamiseks mõeldud protseduurid on kirjeldatud ISO/IEC direktiivide 1. osas. Eriti tuleb silmas pidada eri heakskiidukriteeriume, mis on vajalikud eri liiki ISO dokumentide puhul. See dokument on kavandatud ISO/IEC direktiivide 2. osas esitatud toimetamisreeglite järgi (vt www.iso.org/directives või www.iec.ch/members_experts/refdocs).

Tuleb pöörata tähelepanu võimalusele, et standardi mõni osa võib olla patendiõiguse objekt. ISO ei vastuta sellis(t)e patendiõigus(t)e väljaselgitamise ega selgumise eest. Dokumendi väljatöötamise käigus väljaselgitatud või selgunud patendiõiguste üksikasjad on esitatud sissejuhatuses ja/või ISO-le saadetud patendideklaratsioonide loetelus (vt www.iso.org/patents) või IEC-le saadetud patendideklaratsioonide loetelus (vt https://patents.iec.ch).

Mis tahes selles dokumendis kasutatud äriline käibenimi on kasutajate abistamise eesmärgil esitatud teave ja ei kujuta endast toetusavaldust.

Selgitused standardite vabatahtliku kasutuse ja vastavushindamisega seotud ISO eriomaste terminite ja väljendite kohta ning teave selle kohta, kuidas ISO järgib WTO tehniliste kaubandustõkete lepingus sätestatud põhimõtteid, on esitatud järgmisel aadressil: www.iso.org/iso/foreword.html. IEC-s vaata: www.iec.ch/understanding-standards.

Selle dokumendi on koostanud tehnilise komitee ISO/IEC JTC 1 „Information Technology“ alamkomitee SC 27 „Information security, cybersecurity and privacy protection“.

Kolmas väljaanne tühistab ja asendab teist väljaannet (ISO/IEC 27001:2013), mis on tehniliselt läbi vaadatud. See sisaldab ka tehnilisi parandusi ISO/IEC 27001:2013/Cor 1:2014 ja ISO/IEC 27001:2013/Cor 2:2015.

Peamised muudatused on järgmised:

— tekst on viidud kooskõlla haldussüsteemide standardite ühtlusstruktuuriga ja standardiga ISO/IEC 27002:2022.

Igasugune tagasiside ja küsimused selle dokumendi kohta tuleks suunata dokumendi kasutaja rahvuslikule standardimisorganisatsioonile. Täielik loetelu nende organisatsioonide kohta on leitav veebilehtedelt www.iso.org/members.html ja www.iec.ch/national-committees.

SISSEJUHATUS

0.1 Üldist

See dokument 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 selles, et riske hallatakse adekvaatselt.

On tähtis, et infoturbe halduse süsteem oleks organisatsiooni protsesside ja üldise haldusstruktuuri lahutamatu osa ning et infoturvet arvestataks protsesside, infosüsteemide ja juhtimismeetmete kavandamisel. Eeldatavalt mastaabitakse infoturbe halduse süsteemi teostus organisatsiooni vajaduste järgi.

Seda standardit saavad sisemised ja välised pooled kasutada organisatsiooni enda infoturvanõuete täitmise võime hindamiseks.

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 kaasnevate terminite ja määratlustega.

0.2 Ühilduvus muude haldussüsteemide standarditega

See dokument kohaldab ISO/IEC direktiivide 1. osa (ISO konsolideeritud täiendosa) lisas SL määratletud ülataseme struktuuri, jaotiste samaseid pealkirju ja teksti, ühiseid termineid ning keskseid määratlusi ja toetab seeläbi ühilduvust teiste lisa SL kohaldanud haldussüsteemide standarditega.

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 kontrolliks ja käsitluseks. Selles standardis püstitatud nõuded on üldistuslikud ning on mõeldud kohaldatavaiks kõigile organisatsioonidele, olenemata nende tüübist, suurusest või iseloomust. Kui organisatsioon taotleb vastavust sellele standardile, ei tohi ta välistada ühtki peatükkides 4 kuni 10 spetsifitseeritud nõuet.

2 NORMIVIITED

Allpool nimetatud dokumentidele on tekstis viidatud selliselt, et nende sisu kujutab endast kas osaliselt või tervenisti selle dokumendi nõudeid. 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

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

ISO ja IEC hoiavad alal standardimisel kasutamiseks olevaid terminoloogiaandmebaase järgmistel aadressidel:

— ISO veebipõhine lugemisplatvorm: kättesaadav veebilehelt https://www.iso.org/obp/;

— IEC Electropedia: kättesaadav veebilehelt https://www.electropedia.org/

4 ORGANISATSIOONI KONTEKST

4.1 Organisatsiooni ja ta konteksti tundmaõppimine

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

MÄRKUS Nende probleemide otsustamisel toetub organisatsioon sisemise ja välise konteksti väljaselgitamisele, mida käsitleb ISO 31000:2018[5] jaotis 5.4.1.

4.2 Huvipoolte vajaduste ja ootuste tundmaõppimine

Organisatsioon peab välja selgitama

a) infoturbe halduse süsteemi jaoks asjakohased huvipooled;

b) nende huvipoolte nõuded, mis puudutavad infoturvet;

c) nõuded, mida tuleb käsitleda infoturbe halduse süsteemi kaudu.

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