EESTI STANDARD EVS-ISO/IEC 27035-2:2024

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

INFOTEHNOLOOGIA
Infoturvaintsidentide haldus
Osa 2: Juhised infoturvaintsidentidele reageerimise kavandamiseks ja ettevalmistusteks

Information technology
Information security incident management
Part 2: Guidelines to plan and prepare for incident response
(ISO/IEC 27035-2:2023, identical)

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

EESTI STANDARDI EESSÕNA

See Eesti standard on

— rahvusvahelise standardi ISO/IEC 27035-2:2023 ingliskeelse teksti sisu poolest identne tõlge eesti keelde ja sellel on sama staatus mis ümbertrüki meetodil vastu võetud originaalversioonil. Tõlgenduserimeelsuste korral tuleb lähtuda ametlikes keeltes avaldatud tekstidest;

— jõustunud Eesti standardina inglise keeles augustis 2024;

— eesti keeles avaldatud sellekohase teate ilmumisega EVS Teataja 2024. aasta augustikuu 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 Teabering OÜ, standardi on heaks kiitnud EVS/TK 04.

Standardi mõni osa või mõni standardis kirjeldatud lahendus võib olla patendiõiguse objekt. EVS ei vastuta sellis(t)e patendiõigus(t)e väljaselgitamise ega selgumise eest.

Standardi mõnedele sätetele on lisatud Eesti olusid arvestavaid märkusi, selgitusi ja täiendusi, mis on tähistatud Eesti maatähisega EE.

See standard on rahvusvahelise standardi ISO/IEC 27035-2:2023 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 International Standard ISO/IEC 27035-2:2023. 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 35.030

SISUKORD

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 heakskiidukriteeriumeid, mis on eri liiki ISO dokumentide puhul vajalikud. See dokument on kavandatud ISO/IEC direktiivide 2. osas esitatud toimetamisreeglite kohaselt (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 jooksul väljaselgitatud või selgunud patendiõiguste üksikasjad on esitatud peatükis „Sissejuhatus“ ja/või ISO-le saadetud patentide deklaratsioonide loetelus (vt www.iso.org/patents) või IEC-le saadetud patentide deklaratsioonide loetelus (vt https://patents.iec.ch).

Mis tahes 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 ja IEC-s aadressil 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“.

Teine väljaanne tühistab ja asendab esimest väljaannet (ISO/IEC 27035-2:2016), mis on tehniliselt üle vaadatud.

Peamised muudatused on järgnevad:

— muudetud on pealkiri;

— lisatud on uued rollid, sealhulgas intsidentide haldusrühm ja intsidendi koordinaator ning nende kohustused;

— nõrkuste haldamisega seotud sisu on muudetud;

— jaotises 6.7 on lisatud organisatsioonidele soovitatud protsessi sisu;

— peatükis 7on struktuur ümber korraldatud;

— jaotis C.3 on asendatud ühe lõiguga;

— uuendatud on kirjandus.

Kõikide standardisarja ISO/IEC 27035 osade loetelu on leitav ISO ja IEC veebilehtedelt.

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

SISSEJUHATUS

See dokument keskendub infoturvaintsidentide haldamisele, mille ISO/IEC 27000 on määratlenud infoturbe juhtimissüsteemi ühe kriitilise tegevusena.

Organisatsiooni intsidendi haldusplaani ja intsidentideks tegeliku valmisoleku vahel võib olla suur lõhe. Seetõttu käsitleb see dokument tegeliku valmisoleku protseduuride väljatöötamist, tõstmaks kindlustunnet, et organisatsioon ka tegelikult on valmis infoturvaintsidentidele reageerimiseks. Kindlustunne saavutatakse intsidentide haldamisega seotud poliitikate ja plaanidega, samuti protsessidega, millega hallatakse intsidentidele reageerimise rühma moodustamiste ja selle toimivuse täiustamist, kogemuste hindamist ja neist saadud teabe rakendamist.

1 KÄSITLUSALA

See dokument annab juhised, et kavandada ja ette valmistada intsidentidele reageerimist ning võtta arvesse intsidentidele reageerimise käigus saadud kogemusi. Juhised põhinevad infoturvaintsidentide halduse mudeli etappidel „kavandus ja ettevalmistus“ ja „kogemused“, mis on esitatud standardis ISO/IEC 27035-1:2023 jaotistes 5.2 ja 5.6.

Kavanduse ja ettevalmistuse etapi põhipunktid on:

— koostada ja dokumenteerida infoturvaintsidentide halduspoliitikad ning kehtestada tippjuhtkonna kohustumus,

— uuendada infoturvapoliitika, sealhulgas riskijuhtimisega seotud poliitika nii organisatsiooni kui ka süsteemi, teenuste ja võrgu tasemel,

— luua infoturvaintsidendi haldusplaan,

— määrata kindlaks intsidendile reageerimise rühm,

— luua ja säilitada asjakohaseid suhted ja sidemed sise- ja välisorganisatsioonidega,

— tehniline ja muu toetus (sh organisatsiooniline ja käidutugi),

— infoturvaintsidentide halduse koolitused ning teadlikkuse tõstmise nõuanded.

Kogemustest õppimise etapi põhipunktid on:

— parendusvaldkondade tuvastamine,

— vajalike parenduste kindlaks tegemine ja rakendamine,

— intsidendi reageerimisrühma hindamine.

Selles dokumendis antud juhised on üldised ja mõeldud kohaldamiseks kõigile organisatsioonidele, olenemata tüübist, suurusest või olemusest. Organisatsioonid saavad selles dokumendis antud juhiseid kohandada vastavalt organisatsiooni tüübile, suurusele ja äritegevuse iseloomule seoses infoturvariski olukorraga. See dokument kehtib ka infoturvaintsidendi haldusteenuseid pakkuvate väliste organisatsioonide kohta.

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

ISO/IEC 27035-1:2023. Information technology — Information security incident management — Part 1: Principles and process

3 TERMINID, MÄÄRATLUSED JA LÜHENDID

3.1 Terminid ja määratlused

Dokumendi rakendamisel kasutatakse standardites ISO/IEC 27000 ja ISO/IEC 27035-1 esitatud termineid ja määratlusi.