



Justiits- ja Digiministeerium
info@justdigi.ee
Suur-Ameerika 1
10122, Tallinn

Teie 25.05.2026 nr 8-1/4143-1;
JDM/26-0608/-1K

Meie 08.07.2026nr 1.1-11/2256-2

**Justiits- ja digiministri määruse
„Eesti infoturbestandard“
kooskõlastamine**

Lugupeetud proua Pakosta

Rahandusministeerium kooskõlastab justiits- ja digiministri määruse „Eesti infoturbestandard“ järgmiste märkustega.

1. Eelnõu § 4 kasutab mõistet „organisatsiooni juhatus“, kuigi määrus kohaldub küberturvalisuse seaduse tähenduses teenuseosutajatele, kelle hulka kuuluvad ka riigiasutused, kohaliku omavalitsuse üksused ja muud organisatsioonivormid, millel klassikaline juhatus puudub. Kuigi seletuskirjas on selgitatud, et juhatuse all peetakse silmas organisatsiooni kõrgeimat juhtimistasandit (nt asutuse juht, täitevorgan vms), ei tulene see üheselt määruse tekstist.

Teeme ettepaneku täpsustada § 4 sõnastust, kasutades neutraalsemat terminit, nt „organisatsiooni kõrgeim juhtimistasand“, või defineerida „juhatus“ § 2 terminina selliselt, et see hõlmab kõiki küberturvalisuse seaduse subjektide juhtimisvorme.

2. Eelnõus kasutatud mõistete valik ei ole piisavalt ühtne ja pigem on segadust tekitav. Kuigi § 3 lõike 2 kohaselt kasutatakse mõistet „infoturbejuht“, ei kasutata seda mõistet järjepidevalt ei eelnõus tervikuna ega seletuskirjas, kus on kasutatud ka teistsugust väljendust „infoturbe eest vastutav isik“. Samuti jääb ebaselgeks, miks on valitud just mõiste „hankejuht“, kuigi seletuskirjas on selgitatud, et vastavaid ülesandeid võivad täita erinevad rollid jääb ikkagi ebaselgeks, miks on vajalik eraldiseisva mõiste kasutamine eelnõus.

Palume eelnõus kasutatud mõisted tervikuna üle vaadata ning tagada nende ühtne ja põhjendatud kasutus. Mõistete valikul tuleb lähtuda kehtivast terminoloogiast ning vältida olukorda, kus sama sisu kirjeldamiseks kasutatakse erinevaid või sisult ebaselgeid mõisteid.

3. Eelnõu § 8 lõike 8 eesmärk on toetada organisatsiooni kohustust hinnata organisatsioonivälise tarneahelaga seotud riske (§ 8 lg 7). Kehtiv sõnastus annab organisatsioonile õiguse nõuda teenusepakujalt tõendusmaterjali, kuid ei rõhuta piisavalt, et hinnangu andmiseks peab organisatsioonil olema ligipääs asjakohasele ja piisavale teabele.

Teeme ettepaneku sõnastada säte järgmiselt:

(8) Organisatsioonivälise tarneahela kaitse vajaduse hindamiseks on organisatsioonil õigus nõuda väliselt osapoolelt kaitsetarbele vastavate turvameetmete rakendamist tõendavat teavet, sealhulgas seirearuandeid, asjakohase käsitusala auditi järeldusotsuseid, turvasertifikaate, enesehindamise tulemusi või muud asjakohast teavet.

4. Määruse lisa 2 punkt 2.4 seab kaugtöö vormis tehtavatele auditiprotseduuridele 30 protsendi ülempiiri. Pilvteenuste, SaaS-lahenduste, hajustaristu ja väliste teenusepakkujate puhul ei pruugi füüsiline kohalkäik alati anda parimat tõendusväärtust. Mõnel juhul on kvaliteetsem tõendus kättesaadav hoopis turvalise kaugjuurdepääsu, ekraanijagamise, konfiguratsiooni läbivaatuse, logianalüüsi või dokumenteeritud kontrolljälje kaudu.

Meie hinnangul peaks auditi vorm lähtuma tõendusmaterjali piisavusest, mitte järgast protsendipiirist. Seega teeme ettepaneku asendada 30 protsendi piir riskipõhise käsitlusega.

Võimalik sõnastus:

„Auditiprotseduure võib teha kaugtöö vormis, kui auditi eesmärk, käsitusala, riskid ja tõendusmaterjali laad seda võimaldavad ning audiitor saab kujundada piisava ja asjakohase hinnangu. Füüsiline paikvaatlus tehakse ulatuses, mis on vajalik füüsiliste, keskkonna- ja tegevuskohapõhiste kontrollide hindamiseks. Pilvteenuste, hajustaristu ja väliste teenusepakkujate kontrollimisel võib kasutada kaugprotseduure, kui need annavad piisava tõendusväärtuse. Kaugtöö vormis tehtud auditiprotseduurid, nende põhjendus ja piirangud kajastatakse auditiaruandes.“.

Lõpetuseks märgime, et on tervitatav, et eelnõuga lihtsustatakse nõudeid ning muudetakse neid erinevatele organisatsioonidele paremini rakendatavaks. Samas peame oluliseks, et Riigi Infosüsteemi Amet hoiaks ka edaspidi ajakohasena ja kättesaadavana E-ITS rakendamist toetavad juhendmaterjalid, sealhulgas etalonturbe kataloogi moodulites esitatud detailsema käsitluse, mis hõlmab turvameetmete kirjeldusi, tüüpilisi ohte ning soovituslikke lahendusi.

Lugupidamisega

(allkirjastatud digitaalselt)

Jürgen Ligi
rahandusminister

Virge Aasa 5885 1493
Virge.Aasa@fin.ee

Kristi Mürsepp 5885 1397
Kristi.Myysepp@fin.ee