Vabariigi Valitsuse määruse „Vabariigi Valitsuse 9. detsembri 2022. a määruse nr 121 „Võrgu- ja infosüsteemide küberturvalisuse nõuded“ muutmine“ eelnõu seletuskirja lisa

Märkuste tabel

	Märkus	Vastus märkusele
	Rahandusministeerium 23.07.2025 kiri nr 1.1-11/3035-3	
	Rahandusministeerium kooskõlastab Vabariigi Valitsuse 9. detsembri 2022. a määruse nr 121 „Võrgu- ja infosüsteemide küberturvalisuse nõuded“ muutmise eelnõu järgmiste märkustega.	
1.	Võttes arvesse direktiivi eesmärki ning NIS 2 direktiivi lisades välja toodud valdkondade väikeste ja mikroettevõtete mõju üldisele tarneahela ja ühiskonna infoturbe tasemele ning asjaolu, et määruse muudatusega ettevõtte ja organisatsiooni vastutus ei vähene, teeme ettepaneku VKE määratluse asemel kasutada sarnaselt Maksu- ja Tolliameti lähenemisele käibe piirmäärana 40 000 eurot aastas. See on ka karistusseadustikus toodud määr, millest alates võib ettevõtte poolne rikkumine kaasa tuua reaalse valdkonna süüteo menetluse. Sellest lähtuvalt oleks ettevõtte enda huvides, et tal oleks olemas tõenduspõhist sisendit võimaldav ja rikkumisi ärahoidev küberturvalisuse seadusele vastav infoturbe halduse süsteem.	**Antud selgitus** Küberturvalisuse seaduses (KüTS) ja selle alusel antud õigusaktides kasutatakse eelnõus kasutatud piiritlemist, mistõttu ei ole õigusselguse eesmärgil mõistlik antud juhul teistsugust piiritlust kasutusele võtta.

	Märkus	Vastus märkusele
2.	Eelnõus (seletuskirjas) ei ole piisavalt selgitatud ega ole arusaadav, miks on vajalik määruse täiendamisel §-ga 5^1 vajalik kehtestada ja rakendada määruse lisa kujul täiendav „esmaste turvameetmete“ loetelu kõikidele teenuseosutajatele, arvestades, et kehtiv E-ITS ja rahvusvaheline standard ISO/IEC 27001 juba käsitlevad neid teemasid süsteemselt. Seletuskirjas ei selgitata, miks ei piirduta olemasolevate standardite lihtsustatud rakendamisega eelnõuga lisatavas § 3 lõikes 2^1 nimetatud isikutele, vaid pannakse täiendav kohustus kõigile. Seega tekib küsimus, miks kohaldatakse lisa nõudeid ühtmoodi kõikidele teenuseosutajatele, kuigi määruse eelnõu eesmärgi kohaselt on selgelt märgitud, et eelnõu fookus on mikro- ja väikeettevõtjate ning kohaliku omavalitsuse hallatavate asutuste haldus- ja töökoormuse vähendamisel. Leiame, et sel juhul peaks määruse lisa, milles sätestatakse esmased turvameetmed, rakenduma üksnes nendele asutustele ja ettevõtetele, keda eesmärk otseselt puudutab, et nende võrgu- ja infosüsteemidele rakendatud meetmeid saaks lugeda piisavalt vastavuses olevaks küberturvalisuse seadusega.	**Antud selgitus** Esmased turvameetmed on nö baastase, mida peavad kõik KüTS subjektid järgima. Ettevõtja või asutus (edaspidi koos ka *organisatsioon*), kes järgib Eesti infoturbestandardit (E-ITS) või rahvusvahelist standardit ISO/IEC 27001 ei pea eraldi esmaseid turvameetmete rakendamist fikseerima, kuivõrd E-ITS ja ISO/IEC 27001 eeldavad selle rakendamist ehk mahukamate nõuete täitmisel on täitetud ka esmased turvameetmed. Kui esineb valdkondi, mida rahvusvaheline standard ISO/IEC 27001 ei käsitle, siis tõesti peab teenuse osutaja rakendama asjakohaseid esmaseid turvameetmeid. Näiteks rahvusvaheline standard ISO/IEC 27001 ei käsitle digitaalset allkirjastamist, mis samas on Eestis laialdaselt kasutusel.
3.	Selgelt on alahinnatud mitme kavandatava turvameetme mõju ja rakendamise keerukus. Seejuures puudub lisa rakendamisega kõikidele teenuseosutajatele pandava mastaapse täiendava halduskoormuse analüüs	**Antud selgitus** Eelnõuga vähendatakse, mitte ei tõsteta ettevõtjate halduskoormust. Nimelt on E-ITS järgimine mahukam kui esmasete turvameetmete rakendamine. Seega esmastele turvameetmetele üleminek vähendab halduskoormust. Samuti ei pea esmaseid turvameetmeid eraldi fikseerima valdkondades kus rakendatakse E-ITSi või rahvusvahelist standardit ISO/IEC 27001 (vt ka punkt 2 vastust).

	Märkus	Vastus märkusele
4.	Hindamata on määruse mõjud eelarvele, sh ei ole hinnatud millist töömahtu ja kulusid toob kaasa esmaste turvameetmete kasutusele võtmine ja edaspidine rakendamine. Samuti mõju kõigile teenuseosutajatele paralleelsete nõuete jälgimise või võrdluses olemasoleva ja kehtivate standarditega. Ehk määruse seletuskirjas ei ole analüüsitud määruse lisa rakendamise tegelikke kulusid ega hinnatud selle mõju teenuseosutajatele, kes on juba E-ITSi rakendanud.	**Antud selgitus** Esmaste turvameetmete rakendamine on osa üldisest küberhügieenist ja võrgu- ja infosüsteemi turvalisest käitamisest, millega peab ettevõtja või asutus arvestama võrgu- ja infosüsteemi ülesehitamisel. Määruse seletuskirja punktides 6.1 ja 6.2 on selgitatud, et esmaste turvameetmete järgimise hindamine võtab aega ca 1-2 tundi. See aeg on oluliselt lühem Eesti infoturbestandardi auditeerimisele kuluvast ajast.
5.	Valla või linna ametiasutuse puhul tuleb vaadata osutatavaid teenuseid ning teenistujate ligipääsu andmekogudele. Praegune seletuskirjas (lk 6, teine lõik) sisalduv selgitus „kui tegemist ei ole andmekogu vastutava töötlejaga või volitatud töötlejaga“ ei ole piisav ja on segadusse ajav, kuna tihti ei pea asutused ja teenistujad end andmekogusid kasutades ja isikute andmeid töödeldes töötlejateks, vaid kasutajateks. Hallatavate asutuste osas kokkuhoiu saavutamiseks on lihtsam käsitleda neid KOV osana ja nõuda, et KOV rakendaks neile enda infoturbe halduse süsteemi.	**Antud selgitus** Andmekogude puhul on andmekogu, selle vastutava töötleja ja volitatud töötleja ning andmeandja olemus ning mõiste kirjas avaliku teabe seaduses (AvTS), ehk: AvTS § 43^1 lg 1: *Andmekogu on riigi, kohaliku omavalitsuse või muu avalik-õigusliku isiku või avalikke ülesandeid täitva eraõigusliku isiku infosüsteemis töödeldavate korrastatud andmete kogum, mis asutatakse ja mida kasutatakse seaduses, selle alusel antud õigusaktis või rahvusvahelises lepingus sätestatud ülesannete täitmiseks.* AvTS § 43^4 lg 1: *Andmekogu vastutav töötleja (haldaja) on riigi- või kohaliku omavalitsuse asutus, muu avalik-õiguslik juriidiline isik või avalikke ülesandeid täitev eraõiguslik isik, kes korraldab andmekogu kasutusele võtmist, teenuste ja andmete haldamist. Andmekogu vastutav töötleja vastutab andmekogu haldamise seaduslikkuse ja andmekogu arendamise eest*. AvTS § 43^4 lg 2: *Andmekogu vastutav töötleja võib volitada andmete töötlemise ja andmekogu majutamise teisele riigi- või kohaliku omavalitsuse asutusele, avalik-õiguslikule juriidilisele isikule või*

	Märkus	Vastus märkusele
		hanke- või halduslepingu alusel eraõiguslikule isikule vastutava töötleja poolt ettenähtud ulatuses. AvTS § 43[4] lg 3: *Volitatud töötleja on kohustatud täitma vastutava töötleja juhiseid andmete töötlemisel ja andmekogu majutamisel ning tagama andmekogu turvalisuse*. AvTS § 43[5] lg 2: *Andmeandjaks on riigi- või kohaliku omavalitsuse asutused või muud avalik-õiguslikud või eraõiguslikud isikud, kui neil on seadusega või selle alusel antud õigusaktiga sätestatud kohustus andmekogusse andmeid esitada või kui nad teevad seda vabatahtlikult.* Kokkuvõtvalt on seega andmekogu volitatud töötleja AvTSi tähenduses üldreeglina selle majutaja. Ning teised kes esitavad õigusaktist või tööülesandest tulenevalt teavet on andmeesitajad või kasutajad. Näiteks võib tuua rahvastikuregistri, mille vastutav töötleja on Siseministeerium. Volitatud töötlejaks on Siseministeeriumi infotehnoloogia- ja arenduskeskus. Kohaliku omavalitsuse asutused ja valitsusasutused on andmeandjad. Andmetele juurdepääs (nt vaatamine) toimub juurdepääsu andmise kaudu või siis andmete väljastamise teel. Andmeandja ja andmetele juurdepääsu omav isik ei ole käsitletavad vastutava ja volitatud töötlejana AvTS tähenduses. Kohaliku omavalitsuse asutuste ja hallatavate asutuste võrgu- ja infosüsteemi korralduse otsustab kohalik omavalitsus, arvestades nende autonoomiat.

Siseministeerium
24.07.2025 kiri nr 1-7/206-4

	Märkus	Vastus märkusele
	Siseministeerium kooskõlastab Vabariigi Valitsuse 9. detsembri 2022. a määruse nr 121 „Võrgu- ja infosüsteemide küberturvalisuse nõuded“ muutmise eelnõu alljärgnevate märkustega:	
1.	Eelnõu „Võrgu- ja infosüsteemide küberturvalisuse nõuded“ Lisa „Esmased turvameetmed“ punkt 7.13 sätestab, et infotehnoloogiaseadmete kaitse valdkonnas peab teenuse osutaja rakendama automaatika- või muu andmesideühendusega seadme kasutamise korral lisaturvameetmeid või keelama seadmes andmeside kasutamise, sealhulgas kaughalduse. Selline sõnastus jääb arusaamatuks. Kas „või muu andmesideühendusega seadme kasutamise korral lisaturvameetmeid või keelama seadmes andmeside kasutamise“ tähendab seadme kasutamise keelamist? Eelnõu seletuskirjas laiem selgitus puudub. Teeme ettepaneku see lisada või p 7.13 täpsustada.	**Antud selgitus** Säte ei eelda seadme kasutamise keelamist vaid ütleb, et kui lisaturvameetmeid ei ole võimalik kasutusele võtta (nt kaughalduse keelamine) või tarvilik rakendada, siis tuleks keelata andmesideühendus. Lahenduseks võib olla ka seadme kasutamine ilma võrguühenduseta ja kaughalduse võimaldamine ainult kindlatel aegadel jne.
2.	Eelnõu seletuskirjas on toodud välja punktides 6.1 ja 6.2, et mikro- ja väikeettevõtjatelt ning vähem kui 50 töötajaga kohalike omavalitsuste hallatavatelt asutustelt ja riigimuuseumitelt ei nõuta Eesti infoturbestandardi või standardi ISO/IEC, sh auditite läbiviimist. Sellest lähtuvalt palume täpsustada, kuidas saame eelnimetatud ettevõtete ja organisatsioonide puhul olla kindlad, et vastavad meetmed on rakendatud kui Riigi Infosüsteemi Ametile (edaspidi RIA) ei pea auditi tulemusi esitama. Teiseks tekib andmete jagamisel küsimus, et mille alusel saab E-ITSi täismahus rakendanud asutus olla veendunud meetmete rakendamises, sest auditi ega välise poole järeldusotsust ei ole. Kas RIA on planeerinud siinkohal täiendavaid maandamismeetmeid?	**Antud selgitus** Riiklik järelevalve ei seisne vaid auditi tulemuste hindamisel Ka käesoleval ajal on ettevõtjaid ja asutusi, kellel on E-ITSi või rahvusvahelise standardi ISO/IEC 27001 järgimiskohustus, kuid puudub auditi läbiviimise kohustus. Küberturvalisuse meetmete järgimise kohustus eelnõukohase määruse jõustumisel ei muutu.

	Märkus	Vastus märkusele
	Sotsiaalministeerium 01.08.2025 kiri nr 1.2-3/1728-2	
	Toetame eelnõus kavandatavaid muudatusi ning teeme ühtlasi täiendava ettepaneku, muuta määruse § 4 selliselt, et auditeerimine oleks edaspidi vabatahtlik. Eelnõus kavandatud § 3 muudatus on hea näide väikeettevõtjaid (sh perearste) puudutavast lahendusest, mis vähendab halduskoormust. Selle valguses teeme ettepaneku muuta ka määruse § 4 vabatahtlikuks ja seda terves ulatuses. Kõik senised kogemused näitavad, et auditeerimise protsessi kulu ja sellesse pandav töömaht ei vasta protsessist saadavale kasule, mistõttu oleks mõistlik see ressurss suunata reaalsete meetmete rakendamisele. Neile asutustele, kes vajavad muudel põhjustel sõltumatut hindamist E-ITS meetmete rakendamisel, tasub võimalus vabatahtlikuna alles jätta. See tähendab, et kui teatud juhtudel on see vajalik, jääb see võimalusena alles – näiteks juhul, kui alternatiivina soovitakse rakendada ISO27001, mille üks kohustuslik osa on ka välise audiitori poolne auditeerimine, et saada sertifikaat. Ettepaneku mõte on kaotada liigne bürokraatia. Audit on kulukas ega loo lisaväärtust kui see ei ole vältimatult vajalik – näiteks neile, kes ei soovi ISO sertifikaati. Samuti lasub vastutus meetmete rakendamise eest ettevõttel ja asutusel, kes peab E-ITSi rakendama ja seda sõltumata sellest, kas auditit rakendati või mitte.	**Antud selgitus** Ettepaneku arvestamine toob kaasa olukorra, kus puudub muu sõltumatu väline osapool, kes saab objektiivselt hinnata, kas turvameetmed on kohaselt rakendatud. Sel juhul jääb ainukeseks „kontrollijaks“ RIA kui järelevalveasutus ja ilmselgelt ei jõua kohe kõikide praeguste kui ka tulevaste (st küberturvalisuse 2. direktiivi tõttu lisanduvate) isikute juurde. Ning jäädakse ainult nö tulekahjusid lahendama. Võib väita, et sarnast temaatikat kontrollib ju ka Andmekaitse Inspektsioon (AKI), kuid ka too asutus ei jõua kõikide järelevalve subjekte ennetavalt külastada. Oleme nõus, et E-ITSi enda meetmed näevad ka ette nö sisekontrolliliste meetmete rakendamise, kuid kui suuremate organisatsioonide juures keegi väline osapool ei ütle, et seda on ka vaja teha, siis on suur on tõenäosus, et seda ei rakendata: Ehk siin on risk, et küberturvalisus jääb tahaplaanile ning sellega tegelemise vajadus ilmneb alles siis, kui mingi suurem sündmus on aset leidnud. Organisatsiooni koosseisus oleva audiitori puhul puudub sõltumatu hindamise aspekt, mis on eriti oluline suure mõjuga organisatsioonide puhul. Samas ülaltoodut arvestades ei ole keeldu organisatsioonil iseseisvalt näha ette siseaudiitori kasutamist kübeturvalisuse hindamisel, mis suute tõenäosusega muudaks sujuvamaks ka koostöö välise audiitoriga.

	Märkus	Vastus märkusele
		Kolmandaks, olukorras, kus asutuses on sisekontroll, siis praktikas ei pruugi siseaudiitoril/-kontrollil olla piisavaid IT- ja küberturvalisuse valdkonna teadmisi, et nendel teemadel silm peal hoida. Siinkohal võib tuua näitena kus Majandus- ja Kommunikatsiooniministeerium langes aastal 2020 andmete õngitsuse ohvriks sõltumata sisekontrolli olemasolust. E-ITSi puhul on ka see asjaolu, et selle koostamisel on võetud eeskuju ka selle alternatiiviks olevast ISO27001'st, mille üks kohustuslik osa on ka välise audiitori poolne auditeerimine, mille tulemusena saadakse ka ISO sertifikaat. Kui selle ettepanekuga nõustuda, siis edaspidiselt ei ole E-ITS ja ISO27001 omavahel vastavuses ning tekitab ka olukorra, kus ühes nõuete kogumis on rohkem kohustuslikke elemente kui teises.
	Eesti Esmatasandi Tervisekeskuste Liit 07.08.2025 kiri	
	/…/ Eesti Esmatasandi Tervisekeskuste Liit (ETTKL)väljendab heameelt, et eelnõus on arvestatud meie varasemate ettepanekutega ning väikese ja keskmise suurusega ettevõtjate (VKE) jaoks on loodud realistlikum ja jõukohasem lähenemine küberturvalisuse nõuete täitmisele. Toetame täielikult muudatust, millega: ● t**äiendatakse määruse § 3 lõikega 2[1]**, mille kohaselt ei kohaldata standardite järgimise ja auditi nõudeid teenuseosutajatele, kellel on majandusaasta jooksul keskmiselt alla 50 töötaja ning aastane käive	**Võetud teadmiseks**

	Märkus	Vastus märkusele
	või bilansimaht ei ületa 10 miljonit eurot (vastavalt Euroopa Komisjoni soovitusele 2003/361/EÜ); ● **tunnistatakse kehtetuks § 4 lõike 4 punkt 1**, millega seni vabastati auditi kohustusest ainult mikroettevõtjad. Eelnõuga kavandatud muudatus kujutab endast sisulist ja arvestavat edasiminekut kehtiva määruse ülesehituses, muutes senise auditipõhise lähenemise selgemaks ja paindlikumaks.	
1.	**Esmased turvameetmed** Mõistame, et kõigile teenuseosutajatele, sealhulgas VKEdele, kohalduvad edaspidi määruse lisas sätestatud esmased turvameetmed. Kuigi üldpõhimõttena on nende kohaldumine mõistetav ja aktsepteeritav, palume täpsustada järgmist: ● Kas VKE-l on lubatud turvameetmete täitmist osaliselt delegeerida, näiteks teenusepakkuja või liitlahenduste kaudu? ● Millisel vormis on oodatud turvameetmete järgimise tõendamine järelevalve käigus (nt logid, protseduuri kirjeldused, riskihinnangud)? ● Kas on kavandatud juhendmaterjalide koostamine, mis aitaksid VKEdel esmaseid turvameetmeid rakendada praktiliselt ja mõistetaval viisil?	**Antud selgitus** Kui organisatsioon ostab sisse mõnd teenust või volitab kedagi teist mõne ülesande tegemiseks, on oluline, et vastastikused kohustused oleks tuvastatavad asjakohasest lepingust (sh võib selliseks lepingu osaks olla mõne teenuse tüüptingimused). Väliste teenuste kasutamine samas ei vabasta organisatsiooni kohustusest hinnata, kas teenus on asjakohane ning kas vastava teenuse jätkuva kasutamine on vajalik või on ka muid variante. Turvameetmete täitmine võib olla tõendatud läbi erinevate tegevuste ja dokumentide. Organisatsioonis kasutatavad turvameetmed võivad olla kajastatud erinevates dokumentides (nt sisekorraeeskiri, arvuti kasutamise juhend jne) Oluline on tagada teabe säilimine ja vajadusel tõendamise võimalus. Samuti peaks olema tagatud olukorra teadlikkuse jätkuvus ning kui vahetub töötaja ei tekiks tammsaarelikku olukorda „*eit mäletas, aga tema suri ära*“.[1]

[1] A.H Tammsaare „Põrgupõhja uus Vanapagan“

	Märkus	Vastus märkusele
		Riigi Infosüsteemi Ameti on avaldanud turvameetmeete rakendamist toetavaid juhiseid ja soovitusi oma veebilehel ning amet uuendab sealset teavet pidevalt. (vt ka https://eits.ria.ee/et/abimaterjalid/veits)
2.	**Logide pidamise kohustus (töö turvalisus)** Tervisekeskused sõltuvad logide kogumisel ja säilitamisel suurel määral IT-teenuse pakkujatest (nt Medisoft, Telia). Praktikas ei pruugi kõik IT-teenuse pakkujad võimaldada lõppkasutajal logidele ligipääsu ega nende eksporti. Palume seetõttu täpsustada: ● Millises ulatuses ja mahus kehtib logide säilitamise kohustus VKE tasandil? ● Kas ja kuidas võetakse järelevalve hindamisel arvesse teenusepakkuja tehnilisi piiranguid ja valmisolekut?	**Antud selgitus** Välise teenuse kasutamisel tuleks tutvuda eelnevalt lepinguga ja veenduda, mil määral ja kuidas teenuse pakkuja salvestab ja säilitab logisid (sh veebipõhiste programmide korral) ning kas see on organisatsioonile piisav. Võimalusel vältida teenuseid, millel logimist ei pakuta. Võib esineda teenuseid, kus teenuse kasutajale ei võimaldata logidele juurdepääsu, kuid samas peaks juurdepääs olema tagatud avaliku korra kaitset või riikliku järelevalvet teostavale ametiasutusele. Kokkuvõtvalt. Logimine võib olla pakutav välise teenuse osutaja poolt, kui tagatud on logide kättesaadavus järelevalve asutuste poolt intsidentide (sh süütegude) menetlemiseks.
3.	**Küberturbeintsidentidest teavitamine (§ 7 ja määruse lisa)** Palume täpsustada: ● Millised intsidendid kvalifitseeruvad teavitamiskohustust käivitavateks? ● Millistest kriteeriumidest peaks VKE lähtuma intsidentide käsitlemisel? ● Kas määruses on ette nähtud proportsionaalne lähenemine olukordades, kus viivitamine teavitamisel on tingitud heausksest eksimusest või vähesest teadlikkusest? ● Millised sanktsioonid võivad kaasneda teavitamisega viivitamisel?	**Antud selgitus** Teavitada võiks igast intsidendist, mille puhul on põhjusta kahtlustada, et selleks mitte õigustatud isik püüab või on saanud juurdepääsu andmetele (sh nö õngitsused) või on sisenenud süsteemi. Samuti tasub teavitada kahtlustest, et mõni võrgu- või infosüsteem ei ole enam turvaline või seda on võimalik ära kasutada teabe saamiseks või teiste isikute vastase ründe teostamiseks. Teavitamine ei tähenda automaatselt järelevalve menetluse algtatamist teavitaja suhtes vaid

	Märkus	Vastus märkusele
		teave võib olla vajalik ka üldise turvalisuse seirel ning üldise turvalisuse tõstmisel.
	ETTKL toetab esitatud muudatusi ning peab eelnõuga kavandatud lähenemist tasakaalustatuks, arvestades VKE-de tegelikke ressursse ja võimekust. Samas rõhutame, et määruse rakendamiseks on oluline tagada suurem õigusselgus teatud tehniliste detailide osas, et vältida ebamõistlikku halduskoormust ning toetada nõuete mõistlikku ja järk-järgulist täitmist.	**Võetud teadmiseks**
	Eesti Haiglate Liit 07.08.2025 kiri nr 154-2B	
	Vabariigi Valitsuse 09. detsembri 2022 määruse nr 121 „Võrgu- ja infosüsteemide küberturvalisuse nõuded“ muutmise eelnõu (edaspidi määruse) ja eelkõige selle lisa 1, on sõnastatud viisil, mis jätab selles sätestatud nõuete sisu tõlgendamise liiga avatuks ning laialivalguvaks. Sõnastuste ebaselgus raskendab nõuete üheselt mõistetavat rakendamist ning tekitab õigusselguse puudumist, eriti arvestades, et tegemist on siduvate ja võimalike järelevalvemeetmete aluseks olevate kohustustega. Tõhusa ja proportsionaalse rakendamise huvides peame oluliseks, et nõuded oleksid selgelt piiritletud, tehniliselt rakendatavad ning üheselt mõistetavad nii haigla kui elutähtsa teenuse osutaja kui ka järelevalveasutuste jaoks.	**Võetud teadmiseks**
	Määruses (seletuskirjas) ei ole piisavalt selgitatud ega ole arusaadav, miks on määruse täiendamisel §-ga 5^1 vajalik kehtestada määruse lisa näol täiendav „esmaste turvameetmete“ loetelu kõikidele teenuse	**Antud selgitus**

	Märkus	Vastus märkusele
	osutajatele. Kehtiv Eesti Infoturbestandard (E-ITS) ja rahvusvaheline standard ISO/IEC 27001 juba käsitlevad neid teemasid süsteemselt. Seetõttu leiame, et määruse lisa, milles sätestatakse esmased turvameetmed, peaks kohalduma üksnes nendele asutustele ja ettevõtetele, keda eesmärk otseselt puudutab, et nende võrgu- ja infosüsteemidele rakendatud meetmeid saaks lugeda piisavalt vastavuses olevaks küberturvalisuse seadusega. Samas peaks nimetatud lisa kohaldumist välistama nende teenuse osutajate suhtes, kes on kohustatud rakendama E-ITS, sh tervishoiuteenuse osutajad kui elutähtsa teenuse osutajad. Määruse seletuskirjas ei ole piisava selgusega lahti kirjeldatud lisa 1 nõuded selliselt, et neist oleks võimalik üheselt aru saada ja nõuete täitmist valideerida.	Esmased turvameetmed on nö baastase, mida peavad kõik KüTS subjektid järgima. Ettevõtja, kes järgib E-ITSi või rahvusvahelist standardit ISO/IEC 27001 ei pea eraldi esmaseid turvameetmete rakendamist fikseerima, kuivõrd E-ITS ja ISO/IEC 27001 eeldavad selle rakendamist ehk mahukamate nõuete täitmisel on täitetud ka esmased turvameetmed. Kui esineb valdkondi, mida rahvusvaheline standard ISO/IEC 27001 ei käsitle, siis tõesti peab teenuse osutaja rakendama asjakohaseid esmaseid turvameetmeid. Näiteks rahvusvaheline standard ISO/IEC 27001 ei käsitle digitaalset allkirjastamist, mis samas on Eestis laialdaselt kasutusel.
	Määrus ja selle lisa tekitavad olulise erinevuse E-ITS kohaldamises tervishoiuteenuse osutaja kui elutähtsa teenuse osutaja poolt. E-ITSi kohaselt valib teenuse osutaja enda tegevuse suhtes kohased turvameetmed, arvestades turbe eesmärke, määratud kaitsetarvet ning standardis sätestatud põhimõtteid. Määruse muudatuse jõustudes senine valikuline ja teenuse osutaja kaalutlusest lähtuv protsess muutub ning rakendub kohustus rakendada vähemalt määruse lisas toodud „esmased turvameetmed“. Selline muutus toob kaasa ka muudatuse küberturvalisuse seadusega ettenähtud teenuse osutaja kohustuste mahus.	**Antud selgitus** Esmaste turvameetmete juures on arvestatud, et tegemist on igapäevase baastasemega, millega ettevõtja peab oma võrgu- ja infosüsteemide rajamisel ning kasutamisel arvestama. E-ITS ja rahvusvaheline standard ISO/IEC on juba järgmine tase ja mõeldud suurema mõjuga ettevõtjatele ning asutustele. Uuele tasemele minnes ei saa asuda seisukohale, et esmased meetmed tuleks „ära unustada“ või vahele jätta. Küll aga ei peaks keskenduma mõnes valdkonnas eraldi esmastele turvameetmetele, kui on rakendatud juba kõrgemaid meetmeid. Baasmeetmete rakendamist võib järgida ka muudes tegevustes. Näiteks eeldab meditsiin, et inimene täidab haigestumise vältimiseks üldtuntud soovitusi hügieeni tagamiseks (käte pesemine jne). Kui juba haigestutakse, siis haiglasse minnes on vastuvõtus esmased (hügieeni)nõuded, arsti kabinetis juba rangemad (hügieeni)nõuded, ravi

	Märkus	Vastus märkusele
		protseduuride või analüüside tegemisel lisanduvad täiendavad (hügieeni)nõuded ning operatsiooni ruumides kõige rangemad (hügieeni)nõuded. See et mõnes haigla ruumis on kasutusel kõrgemad nõuded ei tähenda, et baastaset ei ole vaja järgida või selle järgimist monitoorida. Baastase jääb ikka lähtuvalt ruumi kasutusest. Samuti võib olukorrast lähtuvalt baastase muutuda. Näiteks viiruste leviku korral nõutakse ka patsiendilt suu- ja ninapiirkonda katva maski kandmist või vahetusjalatseid. Kokkuvõtvalt: baastase on vajalik, sest sellest saab ettevõtja või asutus riskipõhiselt edasi minna või ka riskide vähenemisel tagasi tulla.
	Määrus ja selle lisa ei ole läbivalt terminoloogiliselt ühtsed. Sageli kasutatakse sarnase või sama tähendusega mõisteid erinevas sõnastuses. Näiteks kasutatakse üheaegselt mõisteid „võrgu- ja infosüsteemide turvareeglid“ (p 1.2.) ja „infoturbereeglid“ (p 2.1.) või selliseid mõisteid nagu „infotehnoloogiavarad“ (p 1.4.), „infotehnoloogiaseade“ (p 1.5.) või „infotehnoloogiavahend“ (p 2.2.). Viimaste osas on tegemist mõistetega, millel puuduvad legaaldefinitsioonid, nt ka mõistel „küberhügieen“ (p 2.1). Määruses ja selle lisas on väljutud küberturvalisuse seaduses, Vabariigi Valitsuse määruses „Võrgu- ja infosüsteemide küberturvalisuse nõuded“ ning E-ITSis kasutatavatest mõistetest ning kasutusele võetud uued mõisted. Kui E-ITS määratleb turvameetmeid kui põhi-, standard- või kõrgturvameetmeid, siis määruses on kasutatud mõisteid „esmased turvameetmed“ ja „lisaturvameetmed“.	**Arvestatud osaliselt** „Infotehnoloogiavara“ asendatud läbivalt „infotehnoloogiaseadmega“ vastavas käändes. Nõustume, et sõna hügieen ei ole Eesti õiguses defineeritud. Küll saab sellises olukorras abi „Eesti keele ühendsõnastikust“, mille kohaselt hügieen on *arstiteaduse haru, mis käsitleb abinõusid tervise säilitamiseks (eriti puhtuse tähtsust); vastavate meetmete kogum* või *abinõud mis tahes (ametlike) dokumentide, andmete, seadmete vms säilitamiseks ja korrastamiseks*. Küberhügieeni olemust aitab selgitada ka st küberturvalisuse 2. direktiivi selgituspunkt 89, mille kohaselt *elutähtsad ja olulised üksused peaksid kasutusele võtma mitmesugused küberhügieeni põhitavad, näiteks usaldamatuse põhimõtte, tarkvarauuendused, seadme konfiguratsiooni, võrgu segmenteerimise, identiteedi ja juurdepääsu halduse ning kasutajateadlikkuse, ning pakkuma oma*

	Märkus	Vastus märkusele
		töötajatele koolitusi ning suurendama teadlikkust küberohtude, andmepüügi ja inimestega manipuleerimise meetodite kohta. Lisaturvameetmete all on mõeldud teenuse osutaja poolt rakendatavaid täiendavaid asjakohaseid meetmeid. Seejuures ei ole keelatud kasutada selleks ka E-ITS abi, kus meetmed on jaotatud põhi-, standard- või kõrgmeetmeteks, arvestades nende mõju.
	Määruse ja selle lisa osas esineb süstemaatilist ja sõnastuslikku ebaselgust. Määruse seletuskirjas on selgitatud, et § 5^1 lisamise eesmärk on kehtestada teenuse osutajale kohustus **rakendada** määruse lisas toodud „esmaseid turvameetmeid“. Samas sõnastuslikult kohustab määrus teenuse osutajat üksnes „**esmaste turvameetmete rakendamiseks“ ette nägema** üksikasjalikke meetmeid sättes mainitud turbevaldkondades. Seega määruses kasutatud sõnastuses puudub eesmärgina seatav kohustus rakendada määruse lisas nimetatud „esmaseid turvameetmeid“.	**Arvestatud sisuliselt** Vabariigi Valitsuse 09.12.20322 määrusesse nr 121 “Võrgu- ja infosüsteemide küberturvalisuse nõuded” (edaspidi ka *määrus nr 121*) lisatava §-i 5^1 lõike 1 sõnastust muudetud järgmiselt *„(1) Teenuse osutaja peab kasutusele võtma asjakohased esmased turvameetmed järgmistes turbevaldkondades***:“.**
	Määruses ja selle lisas esitatud nõuete osas on kaheldav esitatud nõuete vastavus hea õigusloome tavadele, eeskätt õigusselguse, proportsionaalsuse ja rakendatavuse põhimõtetele. Kohustused on mitmel juhul sõnastatud üldsõnaliselt, ilma piisava määratletuseta, mis ei võimalda normi adressaadil – tervishoiuteenuse osutajal kui elutähtsa teenuse osutajal – mõistlikul viisil hinnata, milline tegevus oleks nõuetele vastav ning milliste meetmete rakendamine tagaks tervishoiuteenuse osutajale seatud kohustuste täitmise. Nõuded on esitatud liiga üldiselt ega võimalda aru saada, millisel viisil ja milliseid meetmeid kasutades on sätestatud nõuded täidetud ja saavutatud sätte eesmärgiga kooskõlas olev käitumine. Minimaalselt tuleb täiendada	**Antud selgitus** Määrusega sätestatakse eesmärk, mida teenuse osutaja peab saavutama asjakohaseid meetmeid rakendades. Võrgu- ja infosüsteemide, sealhulgas infotehnoloogia rakendamise ulatus ja kasutusalad oma tegevustes on teenuse osutajate osas erinev, mistõttu ei ole võimalik üheselt sobivat piiritlust esitada. On selge, et üksikisikust teenuse osutaja võrguinfosüsteemide kasutus ulatus ja mõju on tunduvalt väiksem kui telekommunikatsiooni teenuseid osutava teenuse osutajal. See aga ei tähena, et kumbki nimetatud ettevõtjatest ei peaks järgima oma võrgu- infosüsteemide kasutamisel esmaseid turvameetmeid,

	Märkus	Vastus märkusele
	seletuskirja ning lahti kirjutada määruses ja selle lisas esitatud nõuete sisu ning vajadusel see varustada näitlikustatud soovitava käitumise kirjeldusega.	sealhulgas küberhügieeni põhimõtteid, küll on erinev meetmete kasutus ja nende ulatus. Näiteks on mõistlik, et mõlemad näevad ette rüperaalidel ekraaniluku olemasolu, kui rüperaal ei ole kasutuses jne.
	Vastavalt määruse § 2 on määrus ja selle lisa kavavandatud jõustuma 1.septembril 2025. Määrus ei näe ette määruse rakendumise erinevust määruse jõustumisest. Selline lühike jõustumise ja rakendamise aeg alahindab kavandatavate kohustuslike turvameetmete mõju ja rakendamise keerukust. Seejuures puudub analüüs määruse ja selle lisa rakendamisega kõikidele teenuse osutajatele kaasneva märkimisväärse täiendava halduskoormuse kohta.	**Antud selgitus** Kavandatava muudatusega ei lisandu teenuse osutajatele täiendavat kohustust võrreldes kehtiva regulatsiooniga. Nii näiteks E-ITSi järgiv ettevõtja peaks olema oma võrgu- ja infosüsteemide kaitsel olema hinnanud eelnõus sätestatud valdkondades ettenähtud esmaste turvameetmete rakendamist asutuses. Ehk E-ITS on olemuselt ulatuslikum kohustus, mis sisaldab juba esmaseid turvameetmeid. Küll muudetakse eelnõuga mõningate teenuse osutajate kohustusi väiksemaks võrreldes kehtiva regulatsiooniga. Seega saab asuda seisukohale, et eelnõuga ei kaasne teenuse osutajatele täiendavat halduskoormust.
	Arvestades, et meetmed on valdavalt sõnastatud liiga üldiselt, on selliselt sõnastatud nõuete täitmiseks mõeldud meetmete hulk vastavuses sellise üldistuse astmega – mida üldisemad on nõuded, seda suurem on nende täitmiseks vajalike turvameetmete hulk. See ei võimalda hoomata turvameetme rakendamise kulu suurust, et tagada sellise üldise nõudega kaasnevate kohustuste eesmärgipärane täitmine ja võimekus vastavaid kulusid kanda.	**Antud selgitus** Rakendada võetavate meetmete vajadus sõltub kasutatavast võrgu- ja infosüsteemist või infotehnoloogia seadmest, seal hulgas nende kasutamise valdkonnast. Seega on kulu sõltuv teenuse osutaja soovist kasutada oma teenuse osutajal tehnoloogiat. Määruse eesmärk on öelda, et tehnoloogia kasutamine ei tohi ohtu seada avalikke huvi (nt kriitilise infrastruktuuri sabotaaž teenuse osutaja seadet kasutades) ja teiste isikute õigusi (nt teenuse osutaja kasutuses olevate eriliiki isikuandmete leke).

	Märkus	Vastus märkusele
	Tervishoiuteenuste osutamisel peab tervishoiuteenuse osutamisega kaasnevad täiendavad kulud, sh küberturvalisuse saavutamiseks tervishoiuteenuse osutajale kohustuslikuks rakendamiseks ettenähtud meetmete rakendamise kulu olema tervishoiuteenuse osutajale eelarveliste vahenditena tagatud. Tervisekassa poolt eraldatavad rahalised vahendid ei arvesta tervishoiuteenuse osutajatele kehtestatud kohustuste täitmise kuluga, sh määruse ja selle lisa kohaste turvameetmete rakendamise ja käigushoiu kuludega.	**Antud selgitus** Mistahes seadme või võrgu- ja infosüsteemi kasutusele võtmise ja selle kasutusala otsustab teenuse osutaja. Seega on seadmest tulenev kulu teenuse osutaja otsustada, mitte ei tulene käesolevast määrusest. Käesolev määrus annab nõuded olukorraks, kus teenuse osutaja on otsustanud seadet kasutada teiste isikute andmete töötlemiseks ning võimaldab seadet kasutada elektroonilise side võrgu kaudu, mis on kättesaadav ka teistele isikutele. Näiteks röntgenseadme kasutusele võtmisel on teenuse osutaja otsustada, kas seade töötab võrguühenduseta või saab seadmest edastada teavet ka võrku.
	Määrus ja selle lisa sisaldavad mitmeid nõudeid, mille praktiline rakendatavus on küsitav, mille tegelik mõju turvalisuse tasemele jääb ebamääraseks või mis dubleerivad juba olemasolevaid õigusakte. Näiteks ruumides tuleohutuse tagamise nõue on juba piisavalt ja detailselt reguleeritud tuleohutuse seadusega ning isikuandmete töötlemist ja kaitset reguleerib Euroopa Liidu isikuandmete kaitse üldmäärus ja isikuandmete kaitse seadus. Selliste korduvate või ebamääraselt sõnastatud nõuete lisamine võib vähendada määruse terviklikkust ja tekitada segadust nende kohaldamisel, ilma et see looks sisulist lisaväärtust küberturvalisuse tagamisel.	**Antud selgitus** Punkti sõnastust muudetud järgmiselt: *“9.1. järgima võrgu- ja infosüsteemide kasutusele võtmisel ja kasutamisel tuleohutuse nõudeid;”* Punktiga ei kehtestata lisaks tuleohutuse seaduses ja selle alusel antud õigusaktides sätestatule täiendavaid nõudeid. Küll on sätte eesmärk tuletada teenuse osutajale meelde, et mistahes võrgu- ja infosüsteemi rajamisel ning kasutamisel tuleb läbi mõelda ka tuleohutusega seonduv, sealhulgas kas ruumi kasutatakse eesmärgipäraselt ja seal on läbi mõeldud kuidas toimida õnnetuse korral. Näiteks, kas ruumis on piisav jahutus ning ruumis on asjakohased kustutusvahendid, mis ei riku õnnetuse korral seadmeid jne. Sarnaselt teistele füüsilise turbe meetmetele, ei pruugi tuleohutus olla kajastatud sisemises infotehnoloogia juhendis vaid nõuded võivad olla kajastatud ka muudes

	Märkus	Vastus märkusele
		sisekorraga seotud dokumentides (nt tuleohutuseeskiri vms). Oluline on töötajate teadlikkus meetmetest ja nende rakendamise eesmärkidest.
	Järgnevalt esitame EHLi ettepanekud Vabariigi Valitsuse 9. detsembri 2022. aasta määruse nr 121 „Võrgu- ja infosüsteemide küberturvalisuse nõuded“ lisa täiendamiseks ja muutmiseks.	
1.	**Lisa punkt 1.5 kohaselt peab teenuse osutaja määrama igale infotehnoloogiaseadmele vastutava kasutaja.** Ettepanek muuta sõna „igale“ sõnaks „kõikidele“, kuna sõna „kõikidele“ kasutamine võimaldab seadmetele vastutajaid määrata ka grupeeritult. Samuti teeme ettepaneku eemaldada mõiste „kasutaja“ ning sõnastada punkt 1.5 järgmiselt: *„Määrama kõikidele infotehnoloogiaseadmetele vastutajad.“*	**Arvestatud sisuliselt** Lisa muudetud järgmiselt: *1.5. määrama kasutusel olevale infotehnoloogiaseadmele vastutav kasutaja.*
2.	**Lisa punkt 2.6 kohaselt peab teenuse osutaja kasutajate teadlikkuse ja koolituse valdkonnas hoidma pääsuks vajalikke vahendeid teistele kättesaamatuna, sealhulgas salasõnad ja räsid.** Ettepanek asendada sõna „teistele“ sõnadega „volitamata isikutele“ ja sõnastada punkt 2.6 järgmiselt: *„Hoidma pääsuks vajalikke vahendeid, sealhulgas salasõnu ja räsisid, volitamata isikutele kättesaamatuna.“*	**Arvestatud** Lisa teksti muudetud vastavalt.
	Lisa punkt 2.7 kohaselt peab teenuse osutaja kasutajate teadlikkuse ja koolituse valdkonnas kasutama võrgu- ja infosüsteemis vaid kontrollitud ning arvele võetud andmekandjaid ning keelama kontrollimata või tundmatute infotehnoloogiavahendite kasutamise.	**Arvestatud sisuliselt** Kõike andmekandjad ei ole irdandmekandjad. Ettepanek muudab sätte eesmärki. Küll muudame punkti sõnastust järgmiselt: *„2.7. kasutama võrgu- ja infosüsteemis ainult selleks mõeldud ning heaks kiidetud vahendeid, teenuseid ja süsteeme* :“.

	Märkus	Vastus märkusele
	Ettepanek jätta ära nõue „kontrollimata“, kuna kontrollimise mõistet pole defineeritud. Asendada mõiste „andmekandjaid“ mõistega „irdandmekandjaid“ ning „tundmata“ mõistega „volitamata“. Ettepanek sõnastada punkt 2.7 järgmiselt: *„Kasutama võrgu- ja infosüsteemis ainult arvele võetud irdandmekandjaid ning keelama volitamata infotehnoloogiavahendite kasutamise.“*	
	Lisa punkt 2.8 kohaselt peab teenuse osutaja kasutajate teadlikkuse ja koolituse valdkonnas kasutama infotehnoloogiaseadmeid ja andmekandjaid heaperemehelikult ning mitte jätma neid järelevalveta. Meie hinnangul ei loo see punkt selle määruse ja infoturbe kontekstis lisaväärtust ning sõna „järelevalve“ on liiga kitsatähenduslik. Soovitame kaaluda selle punkti eemaldamist määrusest.	**Jäetud arvestamata** Infoturbe kontekstis on nõue, et infotehnoloogiaseadet järelevalvet täiesti asjakohane. Näiteks lennujaamas rüperaali kasutades ei peaks seda jätma toolile, kui ise minnakse poodlema. Või mõne isiku üksi jätmine ruumi, kus asub kriitilisele teabele juurdepääsu võimaldav või kriitilist funktsiooni täitev infotehnoloogiaseade. Järelevalve mõiste ei ole antud olukorras kitsatähenduslik. Järelevalveta jätmise tulemus ei pruugi olla vaid rüperaalist ilma jäämine vaid ka oht, et seadet kasutatakse andmetele juurdepääsemiseks või võrgu- ja infosüsteemi kahjustamiseks. Seega on kasutajate teadlikkuse tõstmine nimetatud tegevusega kaasnevate ohtude osas asjakohane.
	Lisa punkt 3.4 kohaselt peab teenuse osutaja andmeturbe valdkonnas eelistama digitaalset allkirjastamist olulise teabe kinnitamiseks. Punkti sisu on arusaamatu ja põhjendamatu. Teeme ettepaneku selgitada, millistel juhtudel ja millist digitaalset allkirjastamist on punktis mõeldud või punkt määrusest eemaldada.	**Arvestatud sisuliselt** Lisa sõnastust muudetud järgmiselt: „*3.4. eelistama digitaalset lahendust, mis kinnitab oluliste elektrooniliste andmete päritolu ja terviklust, sealhulgas digitaalset allkirjastamist*;“

	Märkus	Vastus märkusele
		Nõude eesmärk on juhtida teenuse osutaja tähelepanu asjaolule, et teenuse osutamiseks oluliste andmete korral tuleks mõelda, kuidas tagada nende terviklus ja vähendada võimalust teiste isikute poolt andmete omavolilist muutmist, seda mis tahes töötlemise etapis. Teenuse osutajal on võimalik ise valida endale sobiv sertifitseeritud lahend, milleks võib näiteks olla digitaalne allkirjastamine, e-tempel, plokiahel, usaldusteenus jne.
	Lisa punkt 4.1 kohaselt peab teenuse osutaja tarnijate ja väliste teenuste osutajate halduse valdkonnas tundma oma tarnijaid ja väliste teenuste osutajaid ning nende tausta kogu tarneahela ulatuses ning rakendama meetmeid lähtudes riigi koostatud avalikest ohuhinnangutest ja riskianalüüsidest tarnijate kohta. Ettepanek sõnastada punkt ümber vähem absolutiseerivas sõnastuses. Mõiste „tundma“ on ebaselge ning võimatu on nõuet täita kogu tarneahela ulatuses. Ettepanek sõnastada punkt 4.1 järgmiselt: *„Omama ülevaadet oma olulistest tarnijatest ja väliste teenuste osutajatest ning nende taustast. Saadud teabe põhjal tuleb rakendada asjakohaseid turvameetmeid, lähtudes riigi koostatud avalikest ohuhinnangutest ja riskianalüüsidest.“*	**Arvestatud** Eelnõu lisa vastavalt muudetud.
	Lisa punkt 6.1 kohaselt peab teenuse osutaja pilveteenuste ja veebirakenduste kaitse valdkonnas kasutama turvalist ja ajakohastatud veebibrauserit. Nõue on liiga üldistav. Oleme nõus ajakohastatud veebibrauseri kasutamise nõudega, kuid mõiste „turvaline veebibrauser“ on määruses defineerimata, mistõttu tuleks kaaluda nõudest sellisel kujul loobumist või täpsustada, milline on turvaline veebibrauser.	**Antud selgitus** Turvaliseks veebibrauseriks saab pidada brauserit, millel on uuendatud ja kehtivad serdid.

	Märkus	Vastus märkusele
	Lisa punkt 6.3 kohaselt peab teenuse osutaja pilveteenuste ja veebirakenduste kaitse valdkonnas järgima turvalise e-kirjavahetuse põhimõtteid ja vältima tundmatute manuste või hüperlinkide avamist. Haiglate hinnangul ei sobi see nõue seadusloome tasandile, vaid on pigem organisatsioonide sisekordade reguleerida. Tundmatute manuste ja hüperlinkide avamist ei ole võimalik täielikult vältida. Teeme ettepaneku loobuda nõudest määruse tasandil.	**Antud selgitus** Nõustume, et tundmatuid manuseid ja hüperlinke ei saa täielikult vältida. Küll on võimalik töötajate teadlikkuse tõstmisega vähendada võimalikke riske Samas eelnõukohane määrus kohaldub kõigile KüTS subjektidele olenemata suurusest. Sellest tuleneval peab eelnõu suutma „kõnetada“ nii suuri kui ka väikseid ettevõtjaid. Sätte eesmärk on tähelepanud juhtuda, et risk võrgu- ja infosüsteemile või tuleneda ka töötaja e-kirjavahetusest ning need on olnud ka paljude küberintsidentide põhjuseks. Organisatsioonil on vabadus tõesti valida koht ja viis kuidas teave töötajateni viia.
	Lisa punkt 6.5 kohaselt peab teenuse osutaja pilveteenuste ja veebirakenduste kaitse valdkonnas eristama ja vältima ebaturvaliste veebilehtede ja rakendusliideste kasutamist. Haiglate hinnangul ei ole võimalik seda nõuet täita, kuna ei ole defineeritud, milline on ebaturvaline veebileht või rakendusliides ning nende täielik vältimine ei ole organisatsiooniliselt ega tehniliselt võimalik.	**Antud selgitus** Sarnaselt infotehnoloogiavahendi kasutusele võtmisele peaks organisatsioon pilvteenuse ja veebirakenduste kasutusele võtmisel hindala, mis on kaasnevad riskid ja kas pakutav on organisatsiooni (ja tema kasutada olevate andmete) jaoks piisavalt turvaline. Kui organisatsiooni hinnangul ei taga pakutav soovitut, siis tuleks hoiduda nende teenuste kasutamisest ja võtta kasutusele mõni alternatiiv. Samuti saab organisatsioon läbi erinevate meetmete piirata ebaturvaliste või mitteturvaliste veebilehtede ja rakendusliidete kasutamist (nt viirusetõrje, spämmifiltrid). Nõustume, et 100% kindlust ei suudeta saavutada. Samas nii nagu igas valdkonnas toimub ka küberkaitses pidev areng, pakkudes välja uusi kaitselahendusi.
	Lisa punkt 7.3 kohaselt peab teenuse osutaja infotehnoloogiaseadmete kaitse valdkonnas pidama arvestust	**Antud selgitus**

	Märkus	Vastus märkusele
	kasutatava tarkvara, tarkvara nõrkuste ja litsentside üle ning uuendama litsentse õigel ajal. Ettepanek asendada mõiste „nõrkuste“ mõistega „haavatavuste“ (*vulnerability*) ning asendada „õigel ajal“ sõnaga „õigeaegselt“. Ettepanek sõnastada punkt 7.3 järgmiselt: *„Pidama arvestust kasutatava tarkvara, selle haavatavuste ja litsentside üle ning uuendama litsentse õigeaegselt.“*	Eelnõus on arvestatud õigusaktides sätestatuga. Küberturvalisuse 2. direktiivi eesti ja inglise keelse versiooni võrdlusest nähtub, et *vulnerability* on tõlgitud kui *nõrkus*. (vt direktiivi selgitava osa p 58).
	Lisa punkt 7.4 kohaselt peab teenuse osutaja infotehnoloogiaseadmete kaitse valdkonnas kasutama turvalist, usaldusväärset ja kehtiva toega tarkvara, sealhulgas eemaldama infotehnoloogiaseadmetest ja telefonidest tarkvara, mis on aegunud või mida ei kasutata. Haiglates on kliiniliselt kasutusel meditsiiniseadmeid, mis töötavad aegunud tarkvaraga. Nende väljavahetamine ei ole alati tehniliselt (seadme tootja ei toeta tarkvarauuendusi) ja finantsiliselt võimalik ega otstarbekas, sest kulud võivad ulatuda kümnetesse või sadadesse miljonitesse eurodesse. Selliste seadmete turvaliseks kasutamiseks rakendatakse lisaturvameetmeid vastavalt riskianalüüsile. Telefonidest tarkvara eemaldamise nõue on liiga absoluutne ja ilma keskhalduslahenduseta tekitaks ebaproportsionaalselt suure halduskoormuse. Ettepanek sõnastada nõue selliselt, et loobutakse meditsiiniseadmete (vms seadmed) puhul sellest nõudest, kui seadmete turvaliseks kasutamiseks rakendatakse riskianalüüsist tulenevaid lisaturvameetmeid.	**Arvestatud sisuliselt** Eelnõus sõnastust muudetud järgmiselt „*..mis on aegunud ja mida ei kasutata*.“ Nõustume ettepaneku esitajaga, et aegunud tarkvaraga tekkiva riski maandamiseks on lisaks kustutamisele rakendada muid riskimaandamise meetmeid. Lisaks muudame lisa preambulit järgmiselt: • *Teenuse osutaja võib käesolevas lisas sätestatud meetmete puhul rakendada mõnda muud samaväärset riskide vähendamise meedet.* • *Teenuse osutaja ei pea käesolevas lisas sätestatud meedet rakendama, kui meede ei ole asjakohane või rakendatav ning ta on teadlik rakendamata jätmisega kaasnevatest riskidest.*
	Lisa punkt 7.7 kohaselt peab teenuse osutaja infotehnoloogiaseadmete kaitse valdkonnas krüpteerima olulist	**Arvestatud sisuliselt**

	Märkus	Vastus märkusele
	teavet töötleva seadme kõvaketta ja teavet sisaldavad välised kõvakettad ajakohast krüptograafilist meedet kasutades. Nõue on liiga absoluutne. Nõustume, et teatud tööjaamades kasutatavad ja kaasaskantavad salvestusseadmed vajavad krüpteerimist, kuid kõigi salvestusseadmete krüpteerimine ei ole teostatav. Selline nõue suurendab riske toimepidevusele ning tekitab asutustele märkimisväärse administratiivkoormuse ja investeerimisvajaduse. Teeme ettepaneku lubada asutustel lähtuda oma riskihinnangutest krüpteerimise rakendamise vajaduse määramisel.	Muudame lisa preambulit järgmiselt: • *Teenuse osutaja võib käesolevas lisas sätestatud meetmete puhul rakendada mõnda muud samaväärset riskide vähendamise meedet.* • *Teenuse osutaja ei pea käesolevas lisas sätestatud meedet rakendama, kui meede ei ole asjakohane või rakendatav ning ta on teadlik rakendamata jätmisega kaasnevatest riskidest.* Preambuli täiendamise eesmärk on tagasisidest tulenevalt selgemalt välja tuua, et võrgu- ja infosüsteemide käitlemisel tuleb kasutada ka talupojatarkust[2] ja tervet mõistust.[3] Olukorras, kus üks asi ei tööta võib töötada muu lahend ning kui miskit asja ei ole, siis ei saa ka asja suhtes soovitatud meetmeid rakendada jne.
	Lisa punkt 7.12 kohaselt peab teenuse osutaja infotehnoloogiaseadmete kaitse valdkonnas rakendama asjakohaseid lisaturvameetmeid oma serveri kaitsmiseks. Jääb selgusetuks, millised on turvameetmed, millised on rakendamist vajavad lisaturvameetmed ja millised neist on asjakohased.	**Antud seletus** Lisaturvameetmete rakendamise vajadus võib tekkida serveri kasutusalast, samuti võib olla ka tootja andnud soovitusi lisaturvameetmete osas, suhtuvalt serveri kasutusest või siis ka paigutusest.
	Lisa punkt 7.13 kohaselt peab teenuse osutaja infotehnoloogiaseadmete kaitse valdkonnas rakendama automaatika- või muu andmesideühendusega seadme kasutamise korral lisaturvameetmeid või keelama seadmes andmeside kasutamise, sealhulgas kaughalduse.	**Arvestatud sisuliselt** Punkti sõnastust muudetud järgmiselt:

[2] Sõnaveeb: „varasematele põlvkondadele ja talupoeglikule eluviisile omane (elu)tarkus; realistlikul elunägemisel, tervel mõistusel põhinev suhtumine“.

[3] Sõnaveeb: „igapäevaelus kujunenud arukus, realistlik arusaamine asjadest; tegelikkust arvestav, praktiline mõtlemine“.

	Märkus	Vastus märkusele
	Jääb arusaamatuks, mis on automaatikasideühendus ja mis on muu andmesideühendus. Samuti on selgusetu, millised on lisaturvameetmed ja millal tuleb andmeside kasutamine keelata.	*„7.13. rakendama automaatikaseadme või muu andmesideühendusega seadme kasutamise korral lisaturvameetmeid või keelama seadmes andmeside kasutamise, sealhulgas kaughalduse;“.*
	Lisa punkt 8.2 kohaselt peab teenuse osutaja sideühenduste ja võrgu kaitse valdkonnas piirama juurdepääsu avalikust võrgust sisevõrgus olevatele seadmetele, sealhulgas kasutama tulemüüri. Ettepanek sõnastada nõue selgemalt ja arusaadavamalt ning vältida mõistete „avalik võrk“ ja „sisevõrk“ kasutamist. Teeme ettepaneku sõnastada punkt 8.2 järgmiselt: *„Piirama volitamata juurdepääsu infosüsteemidele ja seadmetele väliste võrkude kaudu, kasutades tulemüüri või samaväärset turvalahendust.“*	**Arvestatud** Eelnõu lisa vastavalt muudetud.
	Lõpetuseks esitame tagasiside määruse lisa punktide 3.2, 3.3, 3.5, 3.6, 3.7, 6.2, 7.7, 7.8 ja 7.11 osas. Nimetatud punktides ei ole täpsustatud, milliseid andmeid või teavet soovitakse reguleerida, mistõttu hõlmavad need kõike, sealhulgas avalikku teavet ja avalikke andmeid. Haiglate hinnangul ei ole nõuded sellisel kujul otstarbekad. Juurdepääsuga andmed ja teave on juba reguleeritud isikuandmete kaitse seaduses. Teeme ettepaneku täpsustada sõnastust, milliste andmete ja teabe osas nõudeid tuleb täita, või kaaluda määruses nõuetest sellisel kujul loobumist.	**Antud selgitus** Andmete töötlemise turvalisuse hindamisel ei pea lähtuma vaid andmete juurdepääsuvajadusest (konfidentsiaalsus, sh ärisaladus või eriliigilised isikuandmed, asutusesisene teave jms). Lisaks tuleb meetmete rakendamisel mõelda andmete terviklusele ja käideldavusele ja muudele asjaoludele, mis on olulised organisatsiooni toimimiseks.
Majandus- ja Kommunikatsiooniministeerium		

	Märkus	Vastus märkusele
08.08.2025 kiri nr 2-3/2907		
	Kooskõlastame „Võrgu- ja infosüsteemide küberturvalisuse nõuded“ määruse ning ühtlasi teeme ettepaneku muuta määruse §4 sätteid, muutes selle rakendamise paindlikumaks või alternatiivselt ajakohastada auditeerimisjuhendit. Senised kogemused näitavad, et auditeerimisprotsessi kulud ning kohustus erasektorist teenust sisse osta ja sellele kuluv töömaht ei ole proportsioonis protsessist saadava kasuga. Seetõttu oleks otstarbekas suunata ressursid tegevustesse, millel on kvaliteet ja otsene mõju meetmete rakendamisele. Auditeerimisjuhend ja audiitorettevõtte kasutamise kohustus on sätestatud ettevõtlus- ja infotehnoloogiaministri 16. detsembri 2022. a määrusest nr 101 „Eesti infoturbestandard“ Määruse lisa 3 „Auditeerimisjuhend“ punkt 6.2 – Auditeerimiseks sõlmitakse audiitorettevõttega auditeerimisleping. Auditeerimisjuhendi muutmine võimaldaks lihtsustada protsessi, tõstaks infoturbe kvaliteeti ja vähendaks bürokraatiat, andes õiguse teatud toimingute tegemiseks ka teistele pädevatele isikutele, sealhulgas sõltumatutele siseaudiitoritele. Samuti asutustele, kes vajavad sõltumatut hindamist E-ITS meetmete rakendamisel muudel alustel kui KüTS, tuleks säilitada auditeerimise võimalus vabatahtliku ning paindliku mehhanismina. See tähendab, et juhul kui KüTSi nõuete täitmiseks on auditeerimine vajalik, jääb see võimalus alles, näiteks ISO27001 rakendamise korral, kus sertifikaadi saamiseks on nõutav välise audiitori hinnang. Ettepaneku eesmärk on kaotada liigne bürokraatia ja kulutused, mis ei loo sisulist lisaväärtust ning kvaliteeti osapooltele. Oluline on rõhutada,	**Antud selgitus.** Vt Sotsiaalministeeriumi märkusele antud vastust.

	Märkus	Vastus märkusele
	et auditit ei asendata muu sõltumatu hindamisega – vastutus meetmete rakendamise eest lasub sõltumata auditeerimise olemasolust ettevõttel või asutusel, kes E-ITSi rakendab	
	Eesti Infotehnoloogia ja Telekommunikatsiooni Liit 08.08.2025 kiri nr 6.1-2/96-1	
1.	**Esmaste turvameetmete kohaldamise ulatus** ITL toetab eelnõu eesmärki lihtsustada mikro- ja väikeettevõtjate ning kohaliku omavalitsuse hallatavate asutuste küberturvalisuse tagamise nõudeid ja eelnõuga kavandatavat muudatust, mille kohaselt peavad nimetatud isikud hakkama E-ITS või ISO/IEC 27001 standardi asemel järgima esmaseid turvameetmeid. Samas jääb meile arusaamatuks, miks muudetakse eelnõuga esmased turvameetmed kohustuslikuks kõigile küberturvalisuse seaduse subjektidele ehk ka neile, kellel on kohustus järgida nimetatud standardeid. Eelnõuga väiksemate ettevõtete ja asutuste halduskoormust vähendades suurendatakse seda suuremate jaoks. Standardi rakendamisel peavad küberturvalisuse subjektid üle käima kõik meetmed ning põhjendama, kui nad teatud meedet ei rakenda. Eelnõu jõustumine tooks kaasa selle, et kui ettevõte on otsustanud, et mõni standardi meede ei ole nende jaoks mõistlik, siis tuleb seda meedet (kui see kattub eelnõu lisas toodud esmase turvameetmega) siiski kohaldada ja seda mitte riskihaldusest tulenevalt, vaid sellepärast, et õigusakt sätestab sellise kohustuse.	**Antud selgitus** Kavandatava muudatusega ei lisandu teenuse osutajatele täiendavat kohustust võrreldes kehtiva regulatsiooniga. Nii näiteks E-ITSi järgiv ettevõtja peaks olema oma võrgu- ja infosüsteemide kaitsel olema hinnanud eelnõus sätestatud valdkondades ettenähtud esmaste turvameetmete rakendamist asutuses. Ehk E-ITS on olemuselt ulatuslikum kohustus, mis sisaldab juba esmaseid turvameetmeid. Küll muudetakse eelnõuga mõningate teenuse osutajate kohustusi väiksemaks võrreldes kehtiva regulatsiooniga. Seega saab asuda seisukohale, et eelnõuga ei kaasne teenuse osutajatele täiendavat halduskoormust.

	Märkus	Vastus märkusele
	Teeme ettepaneku kehtestada eelnõuga esmased turvameetmed kohustuslikuna ainult eelnõu § 1 punktis 4 toodud isikutele.	
2.	**Eelnõu jõustumine** Eelnõu jõustumine on planeeritud juba 1. septembriks käesoleval aastal, mis jätab subjektidele väga vähe aega määruse täitmiseks. Kuna nõuete täitmine on tagatud küberturvalisuse seadusest tuleneva järelevalve ja karistustega, siis **teeme ettepaneku kehtestada pikem jõustumise aeg.** Pikem jõustumisaeg on vajalik kindlasti juhul, kui ITL-i ettepanekut käesoleva kirja punktis 1 ei aktsepteerita ehk määruses toodud meetmeid peavad hakkama täitma kõik küberturvalisuse seaduse subjektid, kuna ka standardite järgijad peavad sel juhul hakkama oma vastavust eelnõus toodud meetmetele üle kontrollima.	**Jäetud arvestamata** Eelnõuga ei tekitata teenuse osutajatele täiendavaid kohustusi. (vt ka eelmisele ettepanekule antud selgitust)
3.	Ettepanekud eelnõu seletuskirja kohta **Esiteks teeme ettepaneku lisada eelnõu seletuskirja mõjude peatükki mõju küberturvalisuse teenuse osutajatele**. Hetkel käsitletakse seal ainult mõju eelnõu subjektidele ning põgusalt ka küberkeskkonnale. Samas on oluline välja tuua, et küberturvalisuse teenuseid pakkuvate ettevõtete poolt vaadates väheneb nende hulk, kellele standardile vastavuse alast nõustamist pakkuda.	**Antud selgitus** Eelnõukohase määrusega ei vähendata KüTS subjektide hulka. Kõigilt subjektidelt eeldatakse turvalist võrgu- ja infosüsteemi. Seega saab organisatsioonide nõustamisel metoodika ja meetmete osas endiselt kasutada E-ITSi kui näidet meetmest mida võib organisatsioon rakendada. Juhime tähelepanu, et ka määruse nr 121 kehtiva versiooni kohaselt ei pea E-ITSi rakendama, kui kasutatakse rahvusvahelist standardit ning on ka organisatsioone, kellel standardi vahetu järgimise kohustus puudub.
	Teiseks teeme ettepaneku parandada eelnõu seletuskirja peatüki „Eelnõu vastavus Euroopa Liidu õigusele“ sõnastust. Hetkel on seal kirjas, et eelnõu ei ole seotud Euroopa Liidu õiguse ülevõtmisega.	**Antud selgitus**

	Märkus	Vastus märkusele
	Tegelikkuses on eelnõu väga tugevalt seotud NIS2 direktiivi skoobi defineerimisega – kes on küberturvalisuse seaduse subjektid ja millised kohustused neile rakenduvad.	Eelnõu ei ole seotud kübeturvalisuse 2. direktiivi ülevõtmisega seotud subjektide määratlemisega. Eelnõu on seotud nõuete täitmisega, mida olemasolevad kui ka lisanduvad KüTS subjektid peavad järgima.
4.	**Tagasiside eelnõu lisale „Esmased turvameetmed“** Mitmed eelnõu lisas toodud turvameetmed tekitavad küsimusi ning tunduvad ebamõistlikud. Kui nõuda kõigilt küberturvalisuse subjektidelt selles lisas toodud kõigi nõuete järgimist, siis hakatakse tegelema vastavuse riskidega, mitte tegelike infoturbe riskidega. ITL-i konkreetsemad kommentaarid, küsimused ja ettepanekud eelnõu lisa kohta on toodud käesoleva kirja lisas.	**Antud selgitus** Vt Rahandusministeeriumi punktile 2 antud vastust**.**
5.	**Muud tähelepanekud eelnõu kohta** Eelnõu § 1 punktiga 2 lisatav pilvteenuse mõiste tekitab küsimuse, miks on vaja see täies ulatuses eraldi defineerida. Mõiste on olemas küberturvalisuse seaduses ja seda muudetakse NIS2 direktiivi üle võtva küberturvalisuse seaduse muutmise eelnõuga. Kui eelnõuga muudetavas määruses on oluline rõhutada, et määruse kontekstis on pilvteenus ainult avaliku sektori poolt pakutav teenus, siis ei peaks seda tegema uue definitsiooniga.	**Antud selgitus** KüTSis kasutav termin on “pilvandmetöötlusteenus”. Tolle termini definitsioonist tulenevalt on seotud seda osutava ettevõtja majandustegevusega. Kuna KüTS subjektideks on nii avalik-õiguslikud kui eraõiguslikud juriidilised isikud, siis on mõlema osapoole poolt osutatav või kasutava teenuse kirjeldamiseks vajalik ühtne ja üheselt arusaadav termin, kui kirjeldatakse küberturvalisusega seotud nõudeid, mis laienevad kõigile subjektidele. See tähendab, et eelnõukohane “pilvteenus” hõlmab endas nii 1) eraõigusliku juriidilise isiku pakutava pilvega seotud teenust (*ehk KüTS § 2 punktis 7 olevat “pilvandmetöötlusteenust”*) kui ka 2) avalik-õigusliku juriidilise isiku pakutava pilvega seotud teenust (*ehk selliste andmetöötlusressursside kogumile juurdepääsu võimaldav teenus, mida saab paindlikult jagada ning laiendada võrgu- ja infosüsteemi muutmata ning mida pakub kohaliku omavalitsuse üksus või küberturvalisuse seaduse § 3 lõike 4*

	Märkus	Vastus märkusele
		punktides 12 ja 13 nimetatud asutus või isik). Vastavat terminit sätestamata ei ole ühtset terminit, mis tähendaks mõlema sektoriga seotud teenuseid.
	Lisa: Tagasiside eelnõu lisale „Esmased turvameetmed“	
	Lisa punkt 1.1. „*määrama infoturbe eest vastutava isiku*;“ – selline üldine kohustus vajab läbi mõtlemist. Tekib küsimus, kui vastutavaks isikuks määratakse infoturbejuht, kes paikneb organisatsioonis kuskil mitmeid kihte otsustamistasandist kaugemal ning tal ei ole ka ressursse eraldatud siis, kes ikkagi vastutab.	**Antud selgitus** Sätte eesmärk on anda subjektidele “tõuge”, et nad määraks isiku, kelle tööülesanne oleks võrgu- ja infosüsteemide kasutamisega seonduva järgimine ja vajadusel teiste nõustamine (sh vajaliku teabe või isiku leidmisel). Sarnane nõue on ka näiteks andmekaitse valdkonnas andmekaitsespetsialisti määramine. Kui määramist (ehk edasi volitamist) ei toimu, siis saab lugeda, et vastutavaks isikuks on juht ise. Vastutava isiku määramisega ei vabane organisatsiooni juht vastutusest vaid tegemist on igapäevase tegevuse delegeerimisega. Organisatsiooni juhi vastutus tuleneb tsiviilseadustiku üldosa seadusest (nt § 37), äriseadusest (nt § 315). Organisatsiooni juhi või juhtorgani otsustada on kas ja kui suures ulatuses eraldatakse vastutavale isikule ressursse, sh rahalisi, ja milline on tema tegevuse ulatus (pädevus). Kui organisatsioon otsustab lisaks juhule määrata vastutava isiku, siis Vastutav isiku määramise üks eesmärke on ka juhile anda tagasisidet muudatuste vajadusest, mille põhjal juht või juhtorgan siis saab otsustada kas eraldatakse vahendeid uue jaoks või parandatakse olemasolevat või “lepitakse” riskidega. Ka mitte midagi tegemine on otsus.

	Märkus	Vastus märkusele
	Lisa punkt 1.2. „*välja töötama võrgu- ja infosüsteemide turvareeglid*…“ Kus on defineeritud, mis on „turvareeglid“? Kellele need kehtestatakse?	**Antud selgitus** Viidatud sätte täpne sisu on järgmine: *Infoturbe korralduse valdkonnas peab teenuse osutaja välja töötama võrgu- ja infosüsteemide turvareeglid, sealhulgas infoturbepõhimõtted ning tutvustama neid personalile.* Viidatust tulenevalt on soovituslik, et organisatsioon kehtestaks sisemised (turva)reeglid kuidas kasutada olemasolevat võrgu- ja infosüsteemi. Näiteks kuidas ja kes jagab pääsuõigusi, kuidas toimub uute lahenduste kasutusele võtt, millised on kasutaja kohustused ja õigused süsteemi kasutamisel jne. Samuti tuleks organisatsioonis kehtivaid võrgu- ja infosüsteemi kasutamise põhimõtteid (st ka turvameetmeid) tutvustada kõigile kasutajatele eelkõige oma töötajatele. Töötajate teadlikkuse tõstmine ja hoidmine on üks riskide vähendamise meetmest.
	Lisa punkt 1.5. „*määrama igale infotehnoloogiaseadmele vastutava kasutaja*“. Kas kasutaja peaks määrama pigem igale süsteemile?	**Antud selgitus** Vastuste ulatuse määramine on organisatsiooni otsustada. Samas vaid süsteemipõhine kasutaja viitamine võib kaasa tuua olukorra, kus tähelepanu ei pöörata süsteemi toimimiseks vajalikele seadmetele. Seadme kaotus võib seada ohtu ka võrgu ja infosüsteemi. Seadmele nagu mistahes organisatsiooni varale vastutaja seadmine loob ka suurema võimaluse, et seadme puudust või väärkasutust märgatakse kiiremini.

	Märkus	Vastus märkusele
	Lisa punkti 2 pealkiri ning alampunktide sisu ei lähe kokku. Teeme ettepaneku kas laiendada pealkirja näiteks lisades „ning kasutajaõiguste valdkonnas“ või liigutada kasutajaõiguste/halduse teemad asjakohasesse punkti.	**Arvestatud** Määrusesse nr 121 lisatava § 5^1 lõike 1 punkt 2 sõnastatakse järgmiselt: *„2) kasutajate teadlikkus, koolitus ja kasutajaõigused;“* Sellest tulenevalt muudetakse lisa punkti 2 järgmiselt „*2. Kasutajate teadlikkuse, koolituse ja kasutajaõiguste valdkonnas peab teenuse osutaja:“.*
	Lisa punkt 2.1.“ *tutvustama personalile küberhügieeni- ja infoturbereegleid ning tagama neile vastava koolituse vähemalt ühel korral aastas*“. Mõiste „küberhügieen“ on väga vaieldav, sest (ametlik) definitsioon puudub. Kohustuse sisu peab aga olema nii subjektide kui ka järelvalvaja jaoks üheselt selge. Teiseks on kohustus teha koolitust vähemalt ühel korral aastas nõue, mille peab tehtuks märkima ja mille mõju riskikäitumisele võib olla negatiivne – triviaalseid infoturbe koolitusi võidakse hakata pidama tüütuks kohustuseks, mis kujundab negatiivse hinnangu infoturbe suhtes. Võimalusi tagada/kontrollida töötajate infoturbe teadlikkust on rohkem, kui kord aastas toimuv koolitus. Näiteks võib läbi viia testi ja kui töötaja vastab kõigele õigesti, siis koolitust ta enam läbima ei pea.	**Arvestatud sisuliselt** Punkti 2.1 muudetud järgmiselt: *„2.1. tutvustama personalile küberhügieeni- ja infoturbereegleid, hindama teadmisi ja tagama neile vastava koolituse, vajadusel perioodiliselt;“.* Nõustume, et sõna hügieen ei ole Eesti õiguses defineeritud. Küll saab sellises olukorras abi „Eesti keele ühendsõnastikust“, mille kohaselt hügieen on *arstiteaduse haru, mis käsitleb abinõusid tervise säilitamiseks (eriti puhtuse tähtsust); vastavate meetmete kogum* või *abinõud mis tahes (ametlike) dokumentide, andmete, seadmete vms säilitamiseks ja korrastamiseks*. Küberhügieeni olemust aitab selgitada ka st küberturvalisuse 2. direktiivi selgituspunkt 89, mille kohaselt *elutähtsad ja olulised üksused peaksid kasutusele võtma mitmesugused küberhügieeni põhitavad, näiteks usaldamatuse põhimõtte, tarkvarauuendused, seadme konfiguratsiooni, võrgu segmenteerimise, identiteedi ja juurdepääsu halduse ning kasutajateadlikkuse, ning pakkuma oma*

	Märkus	Vastus märkusele
		töötajatele koolitusi ning suurendama teadlikkust küberohtude, andmepüügi ja inimestega manipuleerimise meetodite kohta. Samuti nõustume võimalusega kontrollida töötajate teadmisi küberohtudest ning -hügieenist vastavate perioodiliste testide kaasabil ning vajadusel suunata töötajaid koolitusele. Koolitused võivad olla ka mõnele töötajate grupile kindla perioodiga, et tagada nende teadmine uutest ohtudest ja nende maandamise meetmetest vms. Perioodiline koolitus aitab ka kaasa teadlikkuse säilimisele. Perioodilist koolitust nõutakse ka näiteks töökollektiivides esmaabiandjalt.
	Lisa punkt 2.7. „*kasutama võrgu- ja infosüsteemis vaid kontrollitud ning arvele võetud andmekandjaid ning keelama kontrollimata või tundmatute infotehnoloogiavahendite kasutamise*.“ Meede ei pruugi olla kõikidel juhtudel ja 100% rakendatav. Näiteks avalik-õiguslik organisatsioon peab teatud ulatuses võimaldama juurdepääse organisatsiooni hallatavale võrgule ja/või süsteemidele ka kasutajatele nende oma seadmetega ja teinekord ka andmekandjatega. Määruse meetme detailsus peab olema sellisel tasemel, et kõik, kes on kohustatud meedet järgima, saavad seda praktikas ka teostada.	**Arvestatud sisuliselt** Lisa punkt 2.7. sõnastatud järgmiselt: *„2.7. kasutama võrgu- ja infosüsteemis ainult selleks mõeldud ning heaks kiidetud seadmeid, teenuseid ja süsteeme;“.* Võrgu- ja infosüsteemi haldaja siiski saab reguleerida, millistel tingimustel ja kas ta lubab ka isiklike seadmete kasutust. Samuti on võimalik eristada töötajate ja väliste isikute õigusi või eraldatud süsteeme (nt sisevõrk ja välisvõrk). Lisaks punkti 2.7. muutmisele täiendatakse lisa preambulit järgmiselt: • *Teenuse osutaja võib käesolevas lisas sätestatud meetmete puhul rakendada mõnda muud samaväärset riskide vähendamise meedet.* • *Teenuse osutaja ei pea käesolevas lisas sätestatud meedet rakendama, kui meede ei ole asjakohane või rakendatav ning ta on teadlik rakendamata jätmisega kaasnevatest riskidest.*

	Märkus	Vastus märkusele
		Preambuli täiendamise eesmärk on tagasisidest tulenevalt selgemalt välja tuua, et võrgu- ja infosüsteemide käitlemisel tuleb kasutada ka talupojatarkust ja tervet mõistust. Olukorras, kus üks asi ei tööta võib töötada muu lahend ning kui miskit asja ei ole, siis ei saa ka asja suhtes soovitatud meetmeid rakendada jne.
	Teeme ettepaneku lisada punkti 2 lõppu uus punkt (2.9) järgmises sõnastuses: „kasutama ainult selleks mõeldud ning heaks kiidetud vahendeid, teenuseid ja süsteeme.“	**Arvestatud sisuliselt** Lisa punkt 2.7. sõnastatud järgmiselt: *„2.7. kasutama võrgu- ja infosüsteemis ainult selleks mõeldud ning heaks kiidetud vahendeid, teenuseid ja süsteeme;“.*
	Lisa punkt 3.1. „*hindama, millised andmed ning võrgu- ja infosüsteemid on vajalikud igapäevaseks kasutamiseks*…“. Igapäevane kasutus ei ole hea määratlus. Teeme ettepaneku kasutada selle asemel sõnastust: „on vajalikud igapäevaste ülesannete ja eesmärkide täitmiseks.“	**Võtame teadmiseks**
	Lisa punkt 4.1. „*tundma oma tarnijaid ja väliste teenuste osutajaid ning nende tausta kogu tarneahela ulatuses ning rakendama meetmeid lähtudes riigi koostatud avalikest ohuhinnangutest ja riskianalüüsidest tarnijate kohta*;“ Seda võib püüda teha ja saab teha teatud piirini, aga seda saab teha maksimum 2-3 tarneahela lüli osas. Kui ahel on pikem, siis see ei ole praktikas teostatav. Suured teenusepakkujad (välismaised korporatsioonid) ei pruugi üldse oma tarneahela kohta infot jagada. Sellest sõnastusest võib muuhulgas välja lugeda, et riik teeb riskianalüüse tarnijate kohta. Kas on läbi mõeldud see nõue ka	**Antud selgitus** Sätte eesmärgiks on, et organisatsioon enne võrgu- ja infosüsteemi või infotehnoloogiavahendi kasutusele võtmist: • mõtleks, kas pakutav teenus ühildub olemasolevate süsteemidega ja vastab oodatavale tulemusele (teenusele esitatavatele nõutele);

	Märkus	Vastus märkusele
	riigihangete kontekstis ja tulemas juhised, kuidas hindamist hankeprotsessis teostada?	• kas teenuse pakkuja on võimeline pakkuma kvaliteetset teenust ka tulevikus, lähtudes nende varasemast ajaloost, näiteks makseajaloost, turul oldud ajast ja töötajate arvust; • milline on teenuse pakkuja ärikultuur - eriti oluline on teenuseandja ärikultuur välismaiste teenuseandja puhul, kus tuleb arvestada õigusruumi (nt privaatsustingimused) eripäradega, võimaliku keelebarjääriga ja ajavööndidega; • kas teenuse pakkujal on olemas vajalik personal ja kvalifikatsioon - kontrolli, kas teenuseandja meeskond on kvalifitseeritud, siinhulgas ka alltöövõtjad; • kas pakutav teenuse vastab turvanõuetele - nt uuri, kas teenuseandjal on ISO/IEC 27001 sertifikaat või kas nad on läbinud E-ITS auditi; • jne. Kindlasti peab ka siin jälgima, milline on organisatsiooni jaoks siin mõistlik tase, milline on teabe kättesaadavus ja usaldusväärsus. Kui teave tarneahelast ei ole kättesaadav, siis võib olla piisav ka teenuspakkuja tüüptingimustes kirjeldatud tutvumine, et veenduda teenuse sobivuses jne.
	Lisa punkt 4.2. „*kokku leppima tarnijatega ja väliste teenuste osutajatega kirjalikult taasesitatavas vormis andmete vahetamiseks vajalikud turvanõuded ning kasutatava teenuse tingimused.*“ Teeme ettepaneku asendada „andmete vahetamiseks vajalikud turvanõuded“ sõnastusega „andmete töötlemise nõuded“.	**Jäetud arvestamata** Eelnõu eesmärk ei ole antud juhul reguleerida organisatsiooni toimimist (andmete töötlemise protsess) vaid tõsta fookusse andmete võrgus töötlemise turvanõuded (tööprotsessi osana). Ehk asutus oleks teadlik, kuidas teine osapool andmeid turvaliselt töötleb.

	Märkus	Vastus märkusele
	Lisa punkt 5.1. „*koolitama personali, kuidas ära tunda intsidente, kuidas tuvastada nende mõju ja ulatust ning kuidas neid vältida ja kuidas intsidentide puhul toimida*;“ Sättes on mitmed asjad kokku pandud, mis võiksid olla eraldi käsitletud. . Esiteks, “personal” viitab üldiselt kõikidele organisatsiooni töötajatele. Kõik töötajad peaksid teadma, mida teha, kui nende arvates toimub midagi kahtlast – keda informeerida, kuidas informeerida. Sarnaselt nagu „kui märkad midagi kahtlast, helista 112, räägi, mis juhtus“. Need inimesed ei pea suutma tuvastada intsidendi mõju või ulatust, vaid peavad teadma, millised on võimalikud küberintsidendid ning kuidas intsidendikahtlustest teavitada. Teine sihtrühm on intsidendi edasise käsitlemisega seotud töötajaid (võib olla ka sisse ostetud teenus), kelle hulgas peab olema inimesi, kes oskavad tuvastada intsidendi ulatust ja hinnata mõju. Teiseks: intsidentide vältimine on ennetav tegevus ja seda katab lisa punkt 2.1.	**Antud selgitus** Oluline on kogu personali teadlikkuse tõstmine. Samas ei pea kogu personal omama ühesugust teadmist, vaid see võib varieeruda lähtuvalt tööülesannetest ja kokkupuutest teabe töötlemisega. Niisamuti võib varieerida teabe kuidas ja keda küberintsidendist teavitada. Näiteks esmatasandi töötajal võib piisata võrgu- ja infosüsteemi toimimise eest vastutava isiku või struktuuriüksuse teavitamisest. Samas ettevõttes, kus teenust ostetakse sisse on võib-olla vajalik ka teadmine mis võib olla mõju ja kuidas toimida intsidendi põhjustatud kahju minimaliseerimiseks. Näiteks töötajad teavad kuidas (ja miks) seadmeid võrgust välja lülitada kuni intsidendi lahendamiseni.
	Lisa punkt 5.2. „*määrama isiku, kes koordineerib intsidentide lahendamist, asjaomaste asutuste ja koostööpartnerite teavitamist ning on nende kontaktisik*“. Teeme ettepaneku lisada siia nimekirja intsidentide registreerimise.	**Jäetud arvestamata** Eesmärk ei ole panna kohustust intsidendi organisatsioonisiseseks registreerimiseks, sest selle otsustab organisatsioon oma vajadustest lähtuvalt. Samas kui küberintsidendist (või selle kahtlusest) teavitatakse RIA-t, siis see registreeritakse küberintsidentide registris.
	Lisa punkt 6.3. „*järgima turvalise e-kirjavahetuse põhimõtteid ja vältima tundmatute manuste või hüperlinkide avamist*“. See on sisuline punkt, mida katavad lisa punktid 1.2 ja 2.1. Kas määruses toodud kohustuslikud meetmed peaksid olema sellises detailsuses, defineerides sisuliselt organisatsiooni turbereegleid? Kui on tegemist väikese organisatsiooniga, kus riskide hindamist ei tehta ning rakendatud turve	**Antud selgitus** Esmased turvanõudes on meetmete baastase. Nagu õigesti märgite nõuded on kohaldatavad nii suurtele kui ka väikestele ettevõtjatele, ehk kui ühele tundub selline tegevus loomulik, siis teisele ei pruugi see olla teadvustanud kuni esimeste suurte intsidentideni. Organisatsiooni poolt

	Märkus	Vastus märkusele
	järgib ette antud nõuete nimekirja, siis on see variant. Suuremas organisatsioonis, kus rakendatakse E-ITSi või ISO27001 standardit, ilmselt mitte.	valitavad meetmed on tõesti organisatsiooni otsustada, kuid meetmed tõenäoliselt on siiski välja töötatud praktikast, kogemusest ja teadmisest lähtuvalt. Seega miks mitte juba varakult teisi teavitada, et ka see valdkond vajab võrgu- ja infosüsteemi kaitsel tähelepanu. (vt ka Eesti Haiglate Liidu sama punkti osas tehtud märkuste vastust)
	Lisa punkt 6.4. „*tutvustama personalile telefoni- ja videokõnede tegemise turbe põhimõtteid*“. Sama kommentaar, mis punktile 6.3	**Antud selgitus** Vaata eelmisele punktile antud vastust.
	Lisa punkt 6.6. „*pidama kasutuses olevate pilvteenuste ja nendega seotud riskide arvestust*.“ Kui nõude sihtrühmaks on väiksed organisatsioonid, siis oleks hea kaaluda selle punkti sõnastust, et mida soovitakse saavutada. Riskide arvestuse pidamine ei peaks olema eesmärgiks omaette.	**Antud selgitus** Punkti eesmärk on juhtida teenuse osutajate tähelepanud, et kasutuses olevate pilvteenuste puhul ei pea riske hindama vaid kasutusele võtmise alustamisel vaid ka järgima pidevalt kas tuleb uut teavet süsteemi kohta. Näiteks pädevate asutust või organisatsioonide või pilvteenuse pakkuja enda ülevaated või hoiatused avastatud turvariskidest. Nagu teistegi meetmete juures peab jääma mõistlikkuse piiridesse, mis on organisatsiooni vaates piisav. Samas juhul, kui organisatsioon ostab võrgu- ja infosüsteemi teenust täies mahus või osaliselt sisse, siis võiks teenuse sisse ostmisel üks osa lepingust olla ka teenust pakkuva isiku kohustus teavitada organisatsiooni, kui talle on teatavaks saanud olulise võrgu- ja infosüsteemiga seotud riskid, mis järel saavad lepingupoolet arutada, mis on edasised tegevused riskide maandamiseks. Oluline on mõte „*tunne ja tea kasutatavat teenust*“.
	Lisa punkt 7 tervikuna – kas määruse loojad oskavad hinnata, milliseid ressursse (raha ja teadmised, sh rakendused ja personal, kes oskab neid	**Antud selgitus**

	Märkus	Vastus märkusele
	asju teostada) läheb nende tegevuste tegemiseks vaja? Võtame näiteks punkti 7.6, kas määrusandjal on teada, mida maksab turvalogide kogumise ülesehitamine ja käigushoidmine? Kas on mõeldud, mis peaks olema selle mõte, kui logisid tegelikult ei monitoorita?	Eelnõu eesmärk on et organisatsioon mõtleks läbi: • milliseid sündmusi logitakse (nt sisselogimised, ebaõnnestunud sisselogimiskatsed, failide muutmine, juurdepääs tundlikele andmetele, võrgu liiklus); • kas logitakse kõiki süsteemi komponente ja rakendusi; • kui kaua logisid säilitatakse; • kus logisid säilitatakse (nt kohapeal, pilves, krüpteeritud andmebaasis) • kuidas tagatakse logide terviklus; • kas logidele on juurdepääs 24/7; • kui kiiresti saab logid kätte hädaolukorras; • kas teenuseandja pakub logide analüüsimise teenust; • kas kasutatakse automaatseid jälgimissüsteeme turvasündmuste tuvastamiseks; • kuidas teatatakse turvasündmustest; Sisse ostetavate teenuse puhul tasub olla teadlik kas ja kuidas teenuse osutaja logib ning kellele on logidele juurdepääs (nt tutvuda tüüptingimustega). Logisid on vaja ennetavalt juhuks kui toimub turvaintsident, võimaldab selgitada, mis toimus. Logi on ka vajalik digikriminalistika komponent.
	Lisa punkt 7.10. „*kavandama meetmed juhuks, kui seade läheb kaotsi, varastatakse või läheb katki*“. Kuna defineerimata on, mis on infotehnoloogiaseade, siis kas ikka tõesti on vaja kõikide seadmete jaoks hakata meetmeid välja töötama? Kui organisatsioon teeb riskide hindamist, siis ta rakendab meetmeid vastavalt oma riskihalduse plaanile.	**Antud selgitus** Märkuse sisu jääb selgusetuks. Ka organisatsiooni korraldus, et töötajad ei pea teavitama organisatsiooni organisatsioonile kuuluva vara kahjustamisest või kadumisest (sh vargus) on organisatsooni sisemine meede (kord). Näiteks töölepingu seaduse § 15 lõige 2 punkt 7 sätestab,

	Märkus	Vastus märkusele
		et töötaja teatab viivitamata tööandjale töötakistusest või selle tekkimise ohust ning võimaluse korral kõrvaldab erikorralduseta takistuse või selle tekkimise ohu ja punkt 8 sätestab, et tööandja soovil teavitab tööandjat kõigist töösuhtega seonduvatest olulistest asjaoludest, mille vastu tööandjal on õigustatud huvi. Seega kui organisatsiooni sisemine kord välistab eelpool nimetatu, siis tegemist on organisatsiooni otsusega, mida hiljem ei saa kanda töötajale. Samas rakendatavate meetmete ulatuse otsustab organisatsioon (nt seadme lukustus, või hoidmine piiratud juurdepääsuga ruumis).
	Lisa punkt 9.3. „*vältima ruumides kõrvaliste isikute liikumist saatjata, eelkõige ruumides, kus hoitakse seadmeid või töödeldakse andmeid*;“ Avalikke teenuseid pakkuvates organisatsioonides võib sellises sõnastuses meede olla mitte teostatav.	**Antud selgitus** Ettepaneku sisu ei ole selge. Eelnõus oleva nõude mõte on tuletada meelde, et organisatsioonis tuleks läbi mõelda, kuidas on korraldatud inimeste, sealhulgas kõrvaliste isikute liikumine majas ning kuidas seejuures kaitstakse organisatsiooni kasutuses olevat teavet. Säte ei keela asutuses looma organisatsioonis ruume kus kõrvaline isik liigub organisatsiooni tööajal saatjata. Samas kui seal töödeldakse andmeid või tundlikud seadmed, siis peaks läbi mõtlema turvameetmed. Näiteks on tervishoiuasutustes tavapärane olukord, kus on ruume, milles kliendid liiguvad saatjata, kuid samas ruumis on andmete töötlemiseks loodud tingimused, et klient ei pääse iseseisvalt andmetele ligi ehk vastuvõtt on eraldatud nii, et klient ei saa arvutile ja andmetele juurdepääsu. Ka nõue, et klient ei jää üksi ruumi või ei või organisatsiooni ruumes viibida väljaspool organisatsiooni tööaega on lisas toodud nõudega kooskõlas.

	Märkus	Vastus märkusele
	Eesti Perearstide Selts 08.08.2025 kiri	
	Ettepanekud määruse sõnastuse kohta	
1.	**Teeme ettepaneku § 5[1] sõnastuses jätta välja sõna „üksikasjalikud“.** Terminite „esmased meetmed“ ja „üksikasjalikud meetmed“ paralleelne kasutus võib tekitada regulatsiooni rakendamisel ebaselgust. Kuna määruse lisa täpsustab rakendatavad meetmed, ei ole lõikes 1 vaja eraldi rõhutada nende üksikasjalikkust.	**Arvestatud sisuliselt** Lisatava §-i 5[1] lõike 1 sõnastust muudetud järgmiselt: *„(1) Teenuse osutaja peab kasutusele võtma asjakohased esmased turvameetmed järgmistes turbevaldkondades***:“.**
2.	Teeme ettepaneku lisada § 5[1] lõike 2 lõppu või lõikena 3 järgmine sõnastus „**Teenuse osutaja võib lõikes 2 sätestatud konkreetse meetme jätta rakendamata juhul, kui see ei ole asjakohane või riskianalüüsi alusel, rakendades vajadusel kompenseerivaid meetmeid“.** Sõnastuse lisamise eesmärk on suurendada määruse paindlikkust ja rakendatavust, võimaldades teenuse osutajal jätta esmaste turvameetmete loetelus nimetatud konkreetse meetme rakendamata juhul, kui see ei ole tema tegevuse kontekstis asjakohane või kui riskianalüüs näitab, et selle rakendamine ei ole vajalik (nt juhul, kui risk on muude meetmete abil piisavalt maandatud). Võimaluse rakendada alternatiivseid (nn kompenseerivaid) meetmeid tagaks, et turvameetmete üldine eesmärk – võrgu- ja infosüsteemide kaitse – jääb täidetuks, vältides seejuures olukorda, kus teenuse osutaja peab rakendama meetmeid, mis ei ole tema tegevuse seisukohalt põhjendatud ega proportsionaalsed. Näiteks ei tundu proportsionaalne, et väikeettevõte peaks elektroonikakaupluse tausta kogu tarneahela ulatuses tundma (meetmete p 4.1) või kasutama ekraanilukku või	**Arvestatud sisulisel** Täiendame lisa preambulit. (vt ka Eesti Haiglate Liidu poolt lisa punktile 7.7. tehtud märkusele antud vastust)

	Märkus	Vastus märkusele
	pääsukoodi töötajate ühiskasutuses olevas „nuputelefonis“, mida kasutatakse vaid helistamiseks (meetmete p 7.9).	
3.	Teeme ettepaneku, et §-is 5^1 sätestatud esmaste turvameetmete rakendamise kohustus võiks kohalduda üksnes nende ettevõtjate suhtes, kellele ei kohaldu § 3 lõike 1 lausel antud määrusega sätestatud kohustused. Kahe nõudekomplekti täitmise kohustus suurendab põhjendamatult halduskoormust ning nõuete vahel võib tekkida vastuolusid. E-ITS rakendamisel ei pruugi olla esmased meetmed alati täpselt määruses sõnastatud kujul olla täidetud, kuivõrd sõuete sõnastused ei ole kattuvad ning e-ITS võimaldab ka teatavat paindlikkust.	**Antud selgitus** Esmased turvameetmed on nö baastase, mida peavad kõik KüTS subjektid järgima. Ettevõtja või asutus (edaspidi koos ka *organisatsioon*), kes järgib Eesti infoturbestandardit (E-ITS) või rahvusvahelist standardit ISO/IEC 27001 ei pea eraldi esmaseid turvameetmete rakendamist fikseerima, kuivõrd E-ITS ja ISO/IEC 27001 eeldavad selle rakendamist ehk mahukamate nõuete täitmisel on täitetud ka esmased turvameetmed. Kui esineb valdkondi, mida rahvusvaheline standard ISO/IEC 27001 ei käsitle, siis tõesti peab teenuse osutaja rakendama asjakohaseid esmaseid turvameetmeid. Näiteks rahvusvaheline standard ISO/IEC 27001 ei käsitle digitaalset allkirjastamist, mis samas on Eestis laialdaselt kasutusel.
	Ettepanekud seletuskirja kohta	
1.	Kuna tõdesime, et määruse ja seletuskirja lugejad said regulatsioonist erinevalt aru, palume seletuskirja mõnes aspektis täiendada, et määrus oleks seda rakendama kohustatud isikutele üheselt arusaadav. Teeme ettepanelu tuua seletuskirjas selgemalt välja: - kas „mõlemad tingimused peavad olema täidetud“ selleks, et tekiks E-ITS rakendamise kohustus või vastupidi selleks, et § 5^1 sätestatud nõuete järgimine oleks piisav. Näiteks, kas 60 töötajaga ja 6 miljoni euro suuruse aastakäibega ettevõtja suhtes kohalduvad e-ITS/ISO27001 rakendamise kohustus ning täitmata auditikohustus või mitte;	**Arvestatud** Seletuskirja täiendatud. (Vt ka Ettevõtluse ja Innovatsiooni Sihtasutuse (end EAS) selgitust lk 7, VKE definitsioon)

	Märkus	Vastus märkusele
	- kas väikse suurusega ettevõtjaks kvalifitseeruv elutähtsa teenuse osutaja peab rakendama eITS/ISO27001 ning täitma auditikohustus või piisab § 5^1 sätestatud meetmetest. Meie hinnangul on mõistlik ja proportsionaalne, kui väikse suurusega ettevõtjaks kvalifitseeruva elutähtsa teenuse osutaja puhul piisab § 5^1 sätestatud meetmetest, kuivõrd väikeses organisatsioonis annab lihtsamate ja konkreetsemate nõuete rakendamine meie hinnangul parema lõpptulemuse ning toob kaasa proportsionaalsema ressursikulu ja halduskoormuse.	**Antud selgitus** Kui elutähtsa teenuse osutaja kvalifitseerib mikro- või väikeettevõtjaks, siis ei ole tal nii E-ITSi kui ka rahvusvahelise standardi ISO/IES 27001 järgimise kohustust.
2.	Palume seletuskirjas korrigeerida üldiste turvameetmete hindamise ajakulu hinnangut (p 6.2, järeldus mõju olulisuse kohta). Nõustume, et muudatus vähendab oluliselt väikeettevõtjate halduskoormust, kuid seletuskirjas praegu toodud „1-2 tundi ühe hindamiskorra kohta“ ei ole kaugeltki realistlik – juba näiteks ainuüksi infotehnoloogia varade arvestuse kontrollimine ja uuendamine võtab rohkem aega – ja see on üks kohustusest paljudest. Lisaks näib, et arvestatud ei ole regulaarselt nõutavate tegevustega (näiteks personalikoolitused ja personali juhendamine jms).	**Antud selgitus** Seletuskirjas on tehtud võrdlus auditi läbiviimise ära jätmisega ehk olukorras, kus auditit ei pea läbi viima, kuid selle asemel koostatakse sisemine hindamine, kas nõuded on täidetud ja jätkuvalt asjakohased on muutus märkimisväärne. Mis puudutab nõutavaid tegevusi, siis tegevuste ulatus ja kestus sõltub sarnaselt kehtivatele nõuetele rakendatavatest meetmetest. Küll oleme eeldanud, et esmaste meetmete kehtestamisega ei lange organisatsioonide huvi oma võrgu- ja infosüsteemide, sh andmete kaitsmisel asjakohaste meetmete rakendamiseks ja seeläbi hindasime mõju üldisele küberturvalisusele väikseks.
	Ettepanekud esmaste turvameetmete kohta (määruse lisa)	
	1.5. määrama igale infotehnoloogiaseadmele vastutav kasutaja, <u>kui seade on antud ainult või valdavalt ühe isiku kasutusse.</u> – Põhjendus: ühiskasutuses olevate seadmete puhul on mitu võrdväärset	**Antud selgitus**

	Märkus	Vastus märkusele
	kasutaja, kellele pole administraatori õigusi, ning seadme haldaja (väike ettevõttes on selleks sageli IT-teenuse pakkuja). Vastutava kasutaja määramine ei oleks kuntslik ja ei kajasta tegelikkust. Teenuse osutaja vastutab nii ehk nii oma seadmete eest ning punkti 1.4 kohaselt on tal kohustust pidada kõigi seadmete üle arvestust.	Seadmele vastutaja määramine tagab selle, et seade on kasutuse keskel järelevalve all, see võimaldab tuvastada ka väärkasutamisi. Mistahes töösuhtes eeldatakse, et tööandja tagab tööks vajalike vahendite olemasolu ning lahkumise korral töötaja tagastab töövahendi. Ka kaasvastutuse määramine võib olla asjakohane Näiteks ka ravimite käitlemisel peab ettevõtja määrama isiku, kes vastutab ravimite säilitamise ja transportimise eest, sõltumata sellest et ravimeid väljastavad võibolla kõik töötajad. Siinjuures ei ole piiratud, et selliseid vastutajaid või olla mitu, näiteks ravimiste asukohast või käitlemise nõuetest lähtuvalt. Selline töökorraldus tagab organisatsioonile ülevaate ravimite olemasolust, sealhulgas teabe kas ravimeid on uuendada.
	2.3. kasutama võrgu- ja infosüsteemides personaalseid pääsuõigusi, <u>väjaarvatud juhul, kui süsteem seda mõistlikult ei võimalda.</u> Põhjendus: nt ühiskasutuses oleva EKG-aparaadile vm spetsiifilisele seadmetele ei ole alati võimalik luua erinevaid kasutaja kontosid.	**Antud selgitus** Asjakohane meede võib teie toodud näite puhul olla ka aparaadile ühe kasutajakonto olemasolu, mida uuendatakse pidevalt ning konto andmeid antakse vaid isikutele, kes aparaati tööks vajavad. Sellisel juhul on välistatud selleks mitteõigustatud isikute juurdepääs jms. Lisaks me täpsustame lisa preambulis meetmete rakendamise põhimõtteid. (vt ka Eesti Infotehnoloogia ja Telekommunikatsiooni Liidu poolt lisa punkti 2.7. kohta esitatud märkuse vastust)
	<u>3.4 olulise teabe kinnitamiseks eelistama digitaalset allkirjastamist suulisel või kirjalikku taasesitamist võimaldavale vormile:</u> - Põhjendus: mitmeti mõistetavuse vältimiseks tuleks täpsustada., millega võrreldes tuleks digitaalset allkirjastamist eelistada. Määrus ei	**Anname selgituse** Eelnõu käsitleb võrgu- ja infosüsteemide turvameetmeid, nimetatud süsteemides ei ole käekirjalist allkirjaga teavet kinnitada.

	Märkus	Vastus märkusele
	tohiks kohustada eelistama digitaalset allkirjastamist omakäelisele allkirjastamisele, need on TsÜS § 80 kohaselt võrdsustatud.	(vt ka Eesti Haiglate Liidu poolt lisa punktile 2.7. tehtud märkusele antud vastust)
	3.6. varundama regulaarselt took vajalikke andmeid, hoidma <u>olulisi</u> varundatud andmeid töösüsteemist eraldi ja testima varundatu põhjal <u>oluliste</u> andmete taastamist: - Põhjendus: eraldi asukohta varundamist ja testimist on proportsionaalne nõuda oluliste andmete puhul. Osade andmekategooriate puhul võiks nt *SharePointi / OneDrive* versioonihaldus olla piisav.	**Jäetud arvestamata** Ettepanekust ei selgu, mida on mõeldud „olulisena“. Organisatsioon peaks välja töötama põhimõtted, milliseid andmeid kaitstakse täiendavalt varundamise kaudu. Siinjuures ei saa välistada, et mõningal juhtudel võib see seotud olla ka igapäevase tööga. Ettepaneku esitaja näite korral võib tuua välja, et *Share Pointile* juurdepääsu lõppemisega võib kaduda ka versioonihaldus (nt litsentsi lõpp). Sellises olukorras tuleks organisatsioonil olla valmis, et andmed on kätte saadavad muu varunduse kaudu
	4.1. tundma oma <u>oluliste</u> tarnijaid ja väliste teenuste osutajaid ning nende tausta, <u>kriitiste tarnijate puhul</u> kogu tarneahela ulatuses, ning rakendama meetmeid lähtudes riigi koostatud avalikest ohuhinnangutest ja riskianalüüsidest tarnijate kohta; - Põhjendus ja küsimused: kas mõistame õigesti, et tarnijaks loetakse ka näiteks elektroonikakauplust, kust väikeettevõtja arvuteid ja printereid ostab? Kui nii, siis ei tundu kaugelt proportsionaalne kõigi tarnijate suhtes tarneahela ulatuses taustauuringuid teha. Kui nt elektroonikakauplust ei ole mõeldud tarnija all, siis paluksime näiteks määruse seletuskirjas vm juhendmaterjalis anda tarnija piiritlemise kohta juhiseid. Samuti paluksime võimalusel täpsustada, kas eeldame õigesti, et silmas on peetud konkreetse võrgu- ja infosüsteemidega seotud tarnijaid ja väliste teenuste osutajaid (mitte nt prügiveo teenuse pakkujaid, vee-ettevõtteid jne). Lisaks loodame, et terviseandmete infosüsteemide tarnijad muutuvad iseseisvateks infoturbenõuete ning järelevalve subjektideks.	**Antud selgitus** Ettepanekust ei selgu, mida on mõeldud „olulise“ või „kriitilisena“. Küll tasub siiski organisatsioonil läbi mõelda kust ja kelle kaudu omale vahendeid soetatakse, kas seda tehakse kolmandas riigis oleva veebipoe kaudu või kohaliku esindaja kaudu. Tootjate tausta hindamisel on abiks nii avalikult kättesaadav teave või ka Näiteks Riigi infosüsteemi Ameti poolsed regulaarsed ohuhinnangud või muude asutuste antud hinnangud küberturvalisuse valdkonnas. Iga organisatsiooni hinnata on kui „sügavale“ tarnija või välise teenuse osutaja tausta hindamisega minnakse. Samuti on kasulik reageerida, kui kasutamise ajal on saadud teavet mõne teenuse ebaturvalisuse kohta. Ka teenuse väljast ostmise korral võiks leping sisaldada teavet kuidas käitutakse kui mõni pakutav teenus osutub ebaturvaliseks ehk võrgu- ja infosüsteemi pakkuval

	Märkus	Vastus märkusele
	Väikeettevõtjatest perearstikeskustel puudub kompetents ning võimekus nende üle sisulise järelevalve teostamiseks.	ettevõtjal on oma tegevusalast suurem hoolsuskohtus sellisel teabele reageerimisel kui teenuse kasutajal.
	4.2. kokku leppima oluliste tarnijate ja väliste teenuste osutajatega kirjalikult taasesitatavas vormis konfidentsiaalsete andmete vahetamiseks vajalikud turvanõuded ning kasutatava teenuse tingimused. – Põhjendus: nõue on vajalik ja proportsionaalne juhul, kui tegemist on olulise tarnija/teenusega või vahetatakse konfidentsiaalseid andmeid.	**Anname selgituse** Mistahes ostu-müügi tehingu eelduseks on vastastikune tingimustega nõustumine. Ka juhul kui ostetakse nö valmispakett, siis loetakse isik (tüüp)tingimustega nõustunuks. Ka tüüptingimustes võib olla kirjas kuidas teenuse pakkuja teavet töötleb ning kaitseb, kuidas toimuvad uuendused ja nendest teavitamine. Kui teenuse pakkuja poolsed tingimused organisatsioonile sobivad, siis ei ole ka põhjust teenuse kasutamisest loobuda. Samas on oluline, et organisatsioon omab ülevaadet kuidas tüüptingimused ja nende muudatused on kättesaadavad.
	5.1. koolitama personali, kuidas ära tunda intsidente, ~~kuidas tuvastada nende mõju ja ulatust ning,~~ kuidas neid vältida ja kuidas intsidentide puhul toimida: Põhjendus: väikeettevõttes ei peaks olema intsidentide mõju ja ulatuse tuvastamine tavapersonali ülesanne. Personali tuleks koolitada intsidentide vältimise ja äratundmise osas ning juhendada neid intsidendi korral IT-partnerit/IT-spetsialisti ja infoturbe eest vastutavat isiku teavitama.	**Antud selgitus** Oluline on kogu personali teadlikkuse tõstmine. Samas ei pea kogu personal omama ühesugust teadmist, vaid see võib varieeruda lähtuvalt tööülesannetest ja kokkupuutest teabe töötlemisega. Niisamuti võib varieerida teabe kuidas ja keda küberintsidendist teavitada. Näiteks esmatasandi töötajal võib piisata võrgu- ja infosüsteemi toimimise eest vastutava isiku või struktuuriüksuse teavitamisest. Samas ettevõttes, kus teenust ostetakse sisse on võib-olla vajalik ka teadmine mis võib olla mõju ja kuidas toimida intsidendi põhjustatud kahju minimaliseerimiseks. Näiteks töötajad teavad kuidas (ja miks) seadmeid võrgust välja lülitada kuni intsidendi lahendamiseni.

	Märkus	Vastus märkusele
	7.3. pidama arvestust kasutatav tarkvara, ~~tarkvara nõrkuste~~ ja litsentside üle ning uuendama litsentse õigel ajal; - tarkvara nõrkuste üle arvestuse pidamine ei ole realistlik ega otstarbekas ülesanne. Eert.ee uudiskirjades on igapäev teateid uutest nõrkustest. Pigem on oluline teadaolevatele olulistele nõrkustele vajadusel reageerida (kaetud punktiga 7.4)	**Jäetud arvestamata** Eelnõu koostajate hinnangul on vajalik, et organisatsioon on teadlik kasutatavast tarkvarast ja selle nõrkustest. Ehk kasutusele võtmisel (ja kasutamisel) on teadlikud miks ja milleks on tarkvara võimalik kasutada ja millised on organisatsioonisisesed kasutamise piirangud (nt programmi kasutatakse vaid toetavaks tegevuseks, kuid ärisaladust seal ei töödelda või programm on kasutatav võrguühenduseta jms). Kokkuvõtvalt nõrkustest teadlikkuse omamine on vajalik kasutuse määramisel või vastu meetmete rakendamiseks jne.
	7.4. kasutama turvalist, usaldusväärset ja kehtiva toega tarkvara, sealhulgas eemaldama infotehnoloogiaseadmetest ja telefonidest tarkvara, mis on aegunud või mida ei kasutata. Põhjendatud erandid tuleb dokumenteerida ning vajadusel rakendada turvameetmeid.; - Põhjendus: vahel puuduvad alternatiivid, süsteeme saab vajadusel ülejäänud võrgust eraldada. Ka VEITS juhendab kahtluse korral kaaluma tarkvara väljavahetamist (p 7.4), mitte ei kohusta selleks kõikidel juhtudel.	**Arvestatud sisuliselt** Vt Eesti Haiglate Liidu poolt lisa punkti 7.4. kohta tehtud märkuse vastust.
	7.6. ~~tagama võrgu- ja infosüsteemide ning rakenduste turvasündmuste logimise ja logide kättesaadavus~~: sõnastus asendada järgmiselt: Süsteemide seadistamisel eelistama võimalusel valikuid, mis võimaldavad võrgu- ja infosüsteemide ning rakenduste turvasündmuste logimist ning logide säilitamist vähemalt 90 päeva; - Põhjendus; kättesaadavust ei ole võimalik tagada määratlemata ajaks, väike ettevõtjalt on proportsionaalne nõuda olemasolevate logimisvõimaluste võimalikult head kasutust, mitte agalogihalduse süsteemide kasutuselevõttu. Terviseinfo süsteemidel on	**Jäetud arvestamata** Vt Eesti Infotehnoloogia ja Telekommunikatsiooni Liidu poolt lisa punktile 7 esitatud märkusele antud vastust.

	Märkus	Vastus märkusele
	eraldiseisvad logimisnõuded (tervishoiuteenuse osutamise dokumenteerimise tingimused ja kord § 3^1 lg 2). Kaaluda võib ka lahenduste, et teenuse osutaja enda süsteemides tuleb logisid säilitada fikseeritud aeg ning sisseostetavates süsteemides kasutada ära süsteemi olemasolevad logimisvõimalused.	
	7.9. kasutama tööks vajalikes seadmetes, sealhulgas mobiilseadmetes, mis sisaldavad olulisi või konfidentsiaalseid andmeid, pääsukoodi või ekraanilukku. – Põhjendus: nt ühiskasutuses olevate nuputelefonide puhul, mida kasutatakse asjaajamiseks ei ole nõue asjakohane.	**Antud selgitus** Ka ühiskasutuses olev nuputelefon võib sisaldada teavet, mille vastu võidakse huvi tunda (nt klientide või koostööpartnerite telefoninumbrid). Seega meetmed, mis takistavad andmete kiiret kättesaamist on asjakohased. Ühiskasutuses võib olla ka vastuvõtus kasutatav arvuti, milles registreeritakse klientide külastusi või asutuse üdisele e-postkasti laekunud e-kirju. Sellisel juhul on ekraaniluku kasutamine asjakohane. (Vt ka punkti 2.3. tehtud märkusele antud vastust)
	7.13. rakendama automaatika- või muu andmesideühendusega seadme kasutamise korral lisaturvameetmeid või keelama seadmes andmeside kasutamise, sealhulgas kaughalduse, välja arvatud madala riskiga seadmed: - Põhjendus: näiteks juhtmevabad kõrvaklapid, siir, klaviatuur jms selline ei töötle tundlikku teavet ega võimalda kaugjuhtimist, mistõttu ei ole nende puhul andmeside keelamine otstarbekas ega tehniliselt mõistlik.	**Arvestatud sisuliselt** Punkti sõnastust muudetud järgmiselt: *„7.13. rakendama automaatikaseadme või muu andmesideühendusega seadme kasutamise korral lisaturvameetmeid või keelama seadmes andmeside kasutamise, sealhulgas kaughalduse;“.* Säte ei eelda seadme kasutamise keelamist vaid ütleb, et kui lisaturvameetmeid ei ole võimalik kasutusele võtta (nt kaughalduse keelamine) või tarvilik rakendada, siis tuleks keelata andmesideühendus. Lahenduseks võib olla ka seadme kasutamine ilma

	Märkus	Vastus märkusele
		võrguühenduseta ja kaughalduse võimaldamine ainult kindlates aegadel jne.
	9.1. ja 9.2. „tagamise“ asemel peaks olema kohustus „rakendada meetmeid“ (sarnaselt punktile 9.5). Sel moel oleks kohustuste keelekasutus ühtlasem ning kohustused realistlikumad, keskendudes meetmete rakendamisele, mitte absoluutse tulemuse „tagamisele“, mida ei pruugi olla võimalik igas olukorras garanteerida.	**Arvestatud sisuliselt** Punkte muudetud järgmiselt: *„9.1. järgima võrgu- ja infosüsteemide kasutusele võtmisel ja kasutamisel tuleohutuse nõudeid;* *9.2. jälgima, et ruumi sissepääsud, sealhulgas aknad hoitakse suletuna, kui ruumis ei viibi personali.* *Lisa toodu rakendamisel peab arvestama, et nõuded on esitatud võrgu- ja infosüsteemide osas.“.* Lisaks täiendatud lisa preambulit.
	9.3. vältima tööruumideskõrvaliste isikute liikumist saatjata, eelkõige ruumides, kus hoitakse seadmeid või töödeldakse andmeid: - Põhjendus: nõue ei tohiks kohalduda näiteks ootealade, koridoride, tualettruumi jms suhtes.	**Jäetud arvestamata** Organisatsiooni ruumid, mis on organisatsiooni käsutuses on käsitletavad tööruumidena, mis tõttu muudatus ei too kaasa nõude olemuse muudatust. Eelnõus oleva nõude mõte on tuletada meelde, et organisatsioonis tuleks läbi mõelda, kuidas on korraldatud inimeste, sealhulgas kõrvaliste isikute liikumine majas ning kuidas seejuures kaitstakse organisatsiooni kasutuses olevat teavet. Säte ei keela organisatsioonis ruume, kus kõrvaline isik liigub organisatsiooni tööajal saatjata. Samas kui seal töödeldakse andmeid või tundlikud seadmed, siis peaks läbi mõtlema turvameetmed. Näiteks on tervishoiuasutustes tavapärane olukord, kus on ruume, milles kliendid liigivad vabalt, kuid samas ruumis on andmete töötlemiseks loodud tingimused, mille tulemusel

	Märkus	Vastus märkusele
		klient ei pääse iseseivalt andmetele ligi ehk vastuvõtt on eraldatud nii, et klient ei saa arvutile ja andmetele juurdepääsu, sealhulgas ei näe iseseisvalt töödeldavaid andmeid. Ka nõue, et klient ei jää üksi ruumi või ei või organisatsiooni ruumes viibida väljaspool organisatsiooni tööaega või väljaspool vastuvõtu aega on lisas toodud nõudega kooskõlas.
Eesti Vee-ettevõtjate Liit 08.08.2025 kiri nr 2-/184		
	Eesti Vee-ettevõtete Liit nõustub Vabariigi Valitsuse 9. detsembri 2022. a määruses nr 121 „Võrgu- ja infosüsteemide küberturvalisuse nõuded“ kavandatava muudatusega, mille kohaselt täiendatakse määruse §-i 3 lõikega 2^1 selliselt, et Eesti infoturbestandardi ja rahvusvahelise standardi ISO/IEC 27001 nõudeid ei kohaldata teenuse osutajale, kellel on majandusaasta jooksul keskmiselt alla 50 töötaja ja kelle aastane bilansimaht või aastakäive ei ületa 10 miljonit eurot, arvestades väikeettevõtjate määratlusi Euroopa Komisjoni soovituses 2003/361/EÜ mikro-, väikeste ja keskmise suurusega ettevõtjate määratlemise kohta. Paljud Eesti vee-ettevõtted on mikro- või väikeettevõtted, mistõttu Eesti infoturbestandardi rakendamine, rääkimata rahvusvahelise standardi ISO/IEC 27001 nõuetest, kujuneks nende jaoks ebaproportsionaalselt koormavaks. Selliste standardite täitmine eeldab märkimisväärseid ressursse ning toob kaasa olulised tegevuskulud, mis ei ole väiksemate ettevõtete kontekstis sageli põhjendatud. Seetõttu oleme seisukohal, et väiksematele vee-ettevõtetele tuleb kehtestada	**Võetud teadmiseks**

	Märkus	Vastus märkusele
	diferentseeritud nõuded, mis võtaksid arvesse ettevõtte suurust ja oleksid proportsionaalsed nende võimekusega. Nõustume seisukohaga, et vee-ettevõtted peavad toimepidevuse tagamiseks pöörama olulist tähelepanu küberturvalisuse tagamisele. Leiame, et määruse nr 121 eelnõus kavandatud nõuded esmatasandi turvameetmete rakendamiseks (§ 5^1 ja määruse lisa) on mikro- ja väikeste vee-ettevõtete jaoks piisavad, arvestades nende organisatsioonilist võimekust ja riski profiili.	
	Eesti Linnade ja Valdade Liit 08.08.2025 kiri nr 2-3/88	
	Eesti Linnade ja valdade Liidul (ELVL) hinnangul on määruse eelnõus ebaselgust, mida palume ministeeriumil täpsustada:	
1.	Eelnõu punktiga 2 nähakse ette, et sarnaselt mikro- ja väikeettevõtjatele ei ole vajadust täies ulatuses järgida Eesti infoturbestandardis või standardiga ISO/IEC 27001 sätestatud turvameetmeid valla või linna ametiasutuste hallatavatel asutustel ja osavalla või linnaosa ametiasutuse hallatavatel asutustel, millel on kalendriaasta jooksul keskmiselt alla 50 töötaja. Erand ei laiene vallale või linnale kuuluvale üldhariduskoolile. Samas Küberturvalisuse seaduse paragrahv 3 lõikes 4 täpsustatakse, kellele seaduses teenuse osutaja kohta sätestatut kohaldatakse, sh: 13) valla või linna ametiasutusele, valla või linna ametiasutuse hallatavale asutusele, osavallale, linnaosale, osavalla või linnaosa	**Antud selgitus** KüTS § 3 lõige 1 sätestab valdkonnad, milles tegutsev ettevõtja, või tunnused, millele vastav ettevõtja, on teenuse osutaja. Selles sättes ei ole käsitletud eraldi mikro- või väikeettevõtjat. Ehk sätte kohaselt käsitletakse ettevõtjaid teenuse osutajana sõltumata nende suurusest. KüTS § 7 lõige 5 sätestab Vabariigi Valitsuse või tema volitatud ministri õiguse kehtestada määrusega võrgu- ja infosüsteemide turvameetmetega seotud kohustuste täitmiseks ja süsteemide küberturvalisuse tagamiseks: 1) infoturbe halduse nõuded üldnimetusega Eesti infoturbestandard;

	Märkus	Vastus märkusele
	ametiasutusele, osavalla või linnaosa ametiasutuse hallatavale asutusele ning kohaliku omavalitsuse üksuste ühisametile ja -asutusele; Juhime tähelepanu sellele, et määrusega ei saa erandit kehtestada, kui seaduses puudub sellekohane volitusnorm ja kehtivas seaduses on otsesõnu loetletud, kes seaduse mõistes on teenuse osutaja.	2) turvameetmete üldnõuded; 3) süsteemide turvameetmete erinõuded ja nende kohaldamise ulatuse. Selle volitusnormi raames on Vabariigi Valitsus võtnud kohustuste panemisel arvesse muuhulgas ka ettevõtjate suurus ja tegevuse mõju üldisele kübeturvalisusele. Seejuures ei ole ühtegi teenuse osutajat vabastatud kohustustest täielikult. Sarnaselt ettevõtjatele on eelnõu koostamisel erisuste kehtestamisel kohaliku omavalistuse hallatavate asutustele võetud arvesse muu hulgas asutuste suurust ja tegevuse mõju üldisele küberturvalisusele, sealhulgas kohaliku omavalistuse üksuse raames. Määrusega kavandatav erisus ei piira kohaliku omavalistuse üksusel nõuda oma hallatavatelt asutustelt määruses sätestatust rangemate nõuete täitmisest, sealhulgas auditi läbiviimist.
2.	Eelnõu punktis 7 muudetava määruse § 4 lg 4 p 2 sõnastuse kohaselt ei laiene auditi tegemise kohustus riigimuuseumile, avalik-õigusliku isiku muuseumile, valla või linna ametiasutusele, valla või linna ametiasutuse hallatavale asutusele, osavalla või linnaosa ametiasutusele, osavalla või linnaosa ametiasutuse hallatavale asutusele ning kohaliku omavalitsuse üksuste ühisametile ja -asutusele, kui tegemist ei ole andmekogu vastutava töötlejaga või volitatud töötlejaga. Kui määruse muutmise eesmärk on vabastada koolid auditi tegemise kohustusest, tuleb täpsustada § 4 lõike 4 punkti 2 sõnastust. Praegu on näiteks kõik Tallinna linna haridusasutused, sh koolid ja lasteaiad, Tallinna hariduse infosüsteemi volitatud töötlejad, mistõttu laieneb neile endiselt auditi tegemise kohustus. Seetõttu tuleks määruses selgelt	**Antud selgitus** Eelnõuga lisatavat § 4 lõike 4 punkti 4 täiendatud ühtse arusaamise tagamise eesmärgil järgmiselt: *„…, kui tegemist ei ole andmekogu vastutava töötlejaga või volitatud töötlejaga;“* Küll juhime tähelepanu, et nii riigi, kui kohaliku omavalitsuse hallatava kooli puhul tuleb volitatud ja vastutava töötleja, kasutaja ning andmeandja määratlemisel lähtuda AvTSist. (vt ka Rahandusministeeriumi kirja punktile 5 antud vastust)

	Märkus	Vastus märkusele
	sätestada, et kohaliku omavalitsuse hallatavad koolid, lasteaiad ja huvikoolid on auditi tegemise kohustusest vabastatud, sõltumata sellest, kas nad on vastutavad või volitatud töötlejad.	
3.	3. Praeguses sõnastuses jääb ebaselgeks kohalike omavalitsuste liitude osas: Kui KÜtS §3 lõikes 4 on toodud, et "Käesolevas seaduses teenuse osutaja kohta sätestatut kohaldatakse ka: […] 4) kohaliku omavalitsuse üksusele ja kohaliku omavalitsuse üksuste liidule; Samas nüüd eelnõu ütleb, et subjektid, kes ei pea E-ITSi täismahus rakendama: [...] teenuse osutajale, kellel on majandusaasta jooksul keskmiselt alla 50 töötaja ja kelle aastane bilansimaht või aastakäive ei ületa 10 miljonit eurot, arvestades väikeettevõtjate määratlusi Euroopa Komisjoni soovituses 2003/361/EÜ mikro-, väikeste ja keskmise suurusega ettevõtjate määratlemise kohta (ELT L 124, 20.05.2003, lk 36–41); Kas saame õigesti aru, et kohalike omavalitsuste liidud on selle punktiga hõlmatud, sest nad on 'teenuse osutajad' seaduse mõttes?	**Arvestatud sisuliselt** Nõustume, et Vabariigi Valitsuse 09.12.2022 määruses nr 121 „Võrgu- ja infosüsteemide küberturvalisuse nõuded" on läbivalt teenuse osutajana käsitletud nii KüTS § 3 lõikes 1 loetletud valdkondades tegutsevad ettevõtjad kui ka sama paragrahvi lõikes 4 loetletud juriidilised isikud ja nende üksused. Samas kohaliku omavalitsuse üksuste liitude seaduse § 3 kohaselt võivad üleriigilise kohaliku omavalitsuse üksuste liidu moodustada vaid kohaliku omavalistuse üksused eesmärgiga kaasaaidata kohaliku omavalitsuse üksuste ühistegevuse kaudu kohaliku omavalitsuse üldisele arengule, esindada oma liikmeid ja kaitsta nende ühiseid huve, samuti edendada liikmete koostööd ja luua liikmetele võimalused seadusega ettenähtud ülesannetes paremaks täitmiseks. Seega arvestades ELVL olemust, et saa antud määruse tähenduses teda käsitleda ettevõtjana, küll võib käsitleda samalaadselt esindatavatega kohaliku omavalitsuse üksustega. Arvestades, et ELVL ei ole samastatav kohaliku omavalitsuse üksusega ja tema ülesannetega on Riigi Infosüsteemi Ameti ning Justiits- ja Digiministeeriumi seisukohalt sätestada määruses üheselt arusaadavalt erisus kohaliku omavalitsuse üksuste liitude osas järgmises sõnastuses: *„(2[1]) Käesoleva paragrahvi lõikeid 1 ja 2 ei kohaldata:* */…/*

	Märkus	Vastus märkusele
		4) kohaliku omavalitsuse üksuste liidule, kellel on kalendriaasta jooksul keskmiselt alla 50 töötaja.“
	Eesti Kaubandus-Tööstuskoda 11.08.2025 kiri nr 4/136	
1.	**Erisused mikro- ja väikeettevõtjatele** Kaubanduskoda toetab eelnõu § 1 punkti 4, mille kohaselt ei pea Eesti infoturbestandardis või standardiga ISO/IEC 27001 sätestatud turvameetmeid vahetult kohaldama küberturvalisuse seaduse subjektidest mikro- ja väikeettevõtjad, kellel on majandusaasta jooksul keskmiselt alla 50 töötaja ja kelle aastane bilansimaht või aastakäive ei ületa 10 miljonit eurot. Toetame ka eelnõu § 1 punkti 5, mis vabastab väikeettevõtjad Eesti infoturbestandardi tingimuste täitmise auditi läbi viimise kohustusest.	**Võetud teadmiseks**
2.	**Esmased turvameetmed** Eelnõu § 1 punkt 10 sätestab, et teenuse osutaja on esmaste turvameetmete rakendamiseks kohustatud ette nägema üksikasjalikud meetmed järgmistes turbevaldkondades: infoturbe korraldus; kasutajate teadlikkus ja koolitus; andmeturve; tarnijate ja väliste teenuste osutajate haldus; küberintsidentide haldus; pilvteenuste ja veebirakenduste kaitse; infotehnoloogiaseadmete kaitse; sideühenduste ja võrgu kaitse; füüsiline turve. Kaubanduskoja hinnangul on mõistlik, et esmaseid turvameetmeid peavad kohaldama need mikro- ja väikeettevõtjad, kes vabastatakse	**Antud selgitus** Esmased turvameetmed on nö baastase, mida peavad kõik KüTS subjektid järgima. Organisatsioon, kes järgib Eesti infoturbestandardit (E-ITS) või rahvusvahelist standardit ISO/IEC 27001 ei pea eraldi esmaseid turvameetmete rakendamist fikseerima, kuivõrd E-ITS ja ISO/IEC 27001 eeldavad selle rakendamist ehk mahukamate nõuete täitmisel on täitetud ka esmased turvameetmed. Kui esineb valdkondi, mida rahvusvaheline standard ISO/IEC 27001 ei käsitle, siis tõesti peab teenuse osutaja rakendama asjakohaseid esmaseid turvameetmeid.

	Märkus	Vastus märkusele
	eelnõuga Eesti infoturbestandardis või standardiga ISO/IEC 27001 sätestatud turvameetmete kohaldamisest. Samas jääb meile ebaselgeks, miks peavad esmaseid turvameetmeid järgima ka need ettevõtjad, kes peavad kohaldama Eesti infoturbestandardis või standardiga ISO/IEC 27001 sätestatud turvameetmeid. Kui laiendada esmaste turvameetmete kohaldamist kõikidele teenuse osutajatele, siis sellega suureneb ebamõistlikult nende ettevõtjate koormus ja kulud, kes on kohustatud kohaldama Eesti infoturbestandardis või standardiga ISO/IEC 27001 sätestatud turvameetmeid. Esiteks peavad need ettevõtjad analüüsima, kas nad täidavad määruse lisas esitatud esmaseid turvameetmeid. Kui selgub, et nad ei kohalda kõiki turvameetmeid, siis on neil kohustus teha oma meetmetes vastavaid muudatusi, et nõue oleks täidetud. Samas standardi rakendamisel on teenuse osutajal õigus loobuda mõne meetme kasutamisest, kui ta põhjendab, miks sellise meetme kasutamine ei ole selle ettevõtja vaates mõistlik. Esmaste turvameetmete säte ei näe ette sellist võimalust. Lisaks juhime tähelepanu sellele, et kui määrus jõustub juba 2025. aasta 1. septembril, siis selleks hetkeks ei pruugi kõik teenuse osutajad, kes kohaldavad standardist tulenevaid meetmeid, jõuda oma meetmeid vastavusse viia esmaste turvameetmetega. **Seega Kaubanduskoda teeb ettepaneku muuta eelnõu § 1 punkti 10 sõnastust selliselt, et esmaste turvanõuete kohaldamine on kohustuslik üksnes nendele isikutele, kes vabastatakse eelnõu § 1 punktiga 4 Eesti infoturbestandardis või standardiga ISO/IEC 27001 sätestatud turvameetmete kohaldamisest. Seega ettevõtja,**	Näiteks rahvusvaheline standard ISO/IEC 27001 ei käsitle digitaalset allkirjastamist, mis samas on Eestis laialdaselt kasutusel. Eelnõuga vähendatakse, mitte ei tõsteta ettevõtjate koormust. Nimelt on E-ITS järgimine mahukam kui esmasete turvameetmete rakendamine. Seega esmastele turvameetmetele üleminek vähendab koormust. Samuti ei pea esmaseid turvameetmeid eraldi fikseerima valdkondades kus rakendatakse E-ITSi või rahvusvahelist standardit ISO/IEC 27001. Ühtlasi muudame lisa preambulit järgmiselt. Lisades sinna kaks uut punkti: • *Teenuse osutaja võib käesolevas lisas sätestatud meetmete osas võtta kasutusele mõne muu samaväärse meetme riskide vähendamiseks.* • *Teenuse osutaja ei pea käesolevas lisas sätestatud meedet rakendama, kui meede ei ole asjakohane või rakendatav ning rakendamata jätmisega kaasnevad riskid on teenuse osutaja poolt teadvustatud.* Preambuli täiendamise eesmärk on tagasisidest tulenevalt selgemalt välja tuua, et võrgu- ja infosüsteemide käitlemisel tuleb kasutada ka talupojatarkust ja tervet mõistust. Olukorras, kus üks asi ei tööta võib töötada muu lahend ning kui miskit asja ei ole, siis ei saa ka asja suhtes soovitatud meetmeid rakendada jne.

	Märkus	Vastus märkusele
	kel on kohustus järgida standardist tulenevaid nõudeid, ei peaks kohaldama esmaseid turvanõudeid.	
3.	**Eelnõu lisas sätestatud esmased turvanõuded** Eelnõu lisas on turbevaldkondade kaupa kirjeldatud üksikasjalikke esmaseid turvameetmeid, mida kõik teenuse osutajad peavad rakendama, et subjekti võrgu- ja infosüsteemidele rakendatud meetmed saaks lugeda piisavaks, et olla küberturvalisuse seaduses sätestatud turvanõuetega kooskõlas. Kaubanduskoja hinnangul peavad esmased turvanõuded olema mõistlikud, selged ja arusaadavad ning nende kohaldamine peab olema praktikas võimalik, ilma et sellega kaasneks ebamõistlikult suur koormus või kulu. Oleme saanud ettevõtjatelt tagasisidet, et eelnõu lisas sätestatud esmased turvanõuded vajavad täpsustamist ja muutmist. Toetame Eesti Infotehnoloogia ja Telekommunikatsiooni Liidu kommentaare ja ettepanekuid eelnõu lisa osas.	**Võetud teadmiseks**

Märkuste tabel edastatud märkuste esitajatele e-kirjaga 02.09.2025