Küberturvalisuse seaduse ja teiste seaduste
muutmise seadus (küberturvalisuse 2. direktiivi
üle võtmine) eelnõu seletuskirja
Lisa 2

KAVAND

VABARIIGI VALITSUS
MÄÄRUS

Vabariigi Valitsuse 23. detsembri 1996. a määruse nr 319 „Justiits- ja Digiministeeriumi põhimääruse kinnitamine“, Vabariigi Valitsuse 9. detsembri 2022. a määruse nr 121 „Võrgu- ja infosüsteemide küberturvalisuse nõuded“ ning Vabariigi Valitsuse 3. jaanuari 2024. a määruse nr 1 „Võrgu- ja infosüsteemi turvameetmete nõuded ja nende kohaldamise ulatus pilvteenuse kasutamisel“ muutmine

Määrus kehtestatakse avaliku teabe seaduse § 43 lõike 3, küberturvalisuse seaduse § 7 lõike 5 ja lõike 5 punkti 3 ning Vabariigi Valitsuse seaduse § 42 lõike 1 alusel.

§ 1. Vabariigi Valitsuse 23. detsembri 1996. a määrusega nr 319 „Justiitsministeeriumi põhimääruse kinnitamine” kinnitatud „Justiitsministeeriumi põhimääruse” punkti 54^1 täiendatakse alapunktiga 1^1 järgmises sõnastuses:
„1^1) osaleda Euroopa Parlamendi ja nõukogu direktiivi (EL) 2022/2555, mis käsitleb meetmeid, millega tagada küberturvalisuse ühtlaselt kõrge tase kogu liidus, ja millega muudetakse määrust (EL) nr 910/2014 ja direktiivi (EL) 2018/1972 ning tunnistatakse kehtetuks direktiiv (EL) 2016/1148 (küberturvalisuse 2. direktiiv) (ELT L 333, 27.12.2022, lk 80–152), artiklis 14 nimetatud koostöörühma tegevuses koostöörühma ülesannete kohaselt ja artiklis 16 nimetatud Euroopa küberkriisiga tegelevate kontaktasutuste võrgustikus võrgustiku ülesannete kohaselt.“.

§ 2. Vabariigi Valitsuse 9. detsembri 2022. a määruses nr 121 „Võrgu- ja infosüsteemide küberturvalisuse nõuded” tehakse järgmised muudatused:

1) määruse preambulit täiendatakse pärast sõna „alusel“ lauseosaga „kooskõlas sama paragrahvi lõikega 6“;

2) määruse tekstis asendatakse läbivalt lauseosa „teenuse osutaja“ sõnaga „teenuseosutaja“ vastavas käändes;

3) kolmanda peatüki 1. jagu täiendatakse §-ga 4^1 järgmises sõnastuses:
„**§ 4^1. Alalised turvameetmed**
(1) Teenuseosutaja on alaliste turvameetmete rakendamisel kohustatud:
1) koostama ja rakendama infoturvariskide haldamise metoodika ning protseduurid, sealhulgas analüüsima süsteemi riske, mille käigus koostatakse süsteemi turvalisust ja selle toimepidevust mõjutavate ning küberintsidendi tekkimist põhjustavate riskide loetelu, määratakse riskide realiseerumise tagajärgede raskusaste ja kirjeldatakse riskijuhtimismeetmeid;
2) koostama ja kehtestama infoturbe eesmärgid ning infoturvapoliitika;
3) tagama küberintsidentide käsitlemise protseduuride toimimise;
4) võtma kasutusele abinõud küberintsidendi mõju ja leviku vähendamiseks, sealhulgas vajaduse korral piirama süsteemi kasutamist või juurdepääsu süsteemile;

5) tagama süsteemi toimepidevuse ja kriisihalduse, sealhulgas süsteemi varundus- ja taasteprotseduuride toimimise;
6) tagama süsteemi tarneahela turvalisuse, sealhulgas teenuseosutaja ja tema koostööpartnerite vahelistes lepetes sisalduvate turvameetmetega seotud aspektide regulaarse ülevaatamise ning ajakohastamise;
7) tagama süsteemi hankimise, arendamise ja hooldamise turvalisuse, sealhulgas turvahaavatavuste käsitlemise ning avaldamise;
8) kehtestama turvameetmete regulaarse läbivaatamise, turvameetmete tõhususe hindamise ja infoturbe parendamise protsessi;
9) koolitama regulaarselt kõiki teenuseosutaja ametnikke ja töötajaid küberturvalisuse tagamise osas;
10) kasutama asjakohasel juhul ajakohaseid krüptograafilisi meetmeid;
11) töötama välja ja rakendama personali turvalisuse ning pääsuhalduse põhimõtted ja sellega seotud protseduurid;
12) rakendama varade haldust;
13) kasutama asjakohasel juhul mitmik- või pidevautentimise meetodit või lahendust, turvalise hääl-, video- ja tekstside lahendust ning kriisiolukorras kasutatavat turvalist sidelahendust.
(2) Lõike 1 punktis 6 nimetatud tarneahelaga seotud turvameetmete asjakohasust kaaludes võtab teenuseosutaja arvesse:
1) koostööpartnerile eriomaseid turvahaavatavusi, koostööpartneri toote üldist kvaliteeti ja küberturvalisusega seotud tavasid, sealhulgas toote turvalise arendamise korda;
2) Euroopa Parlamendi ja nõukogu direktiivi (EL) 2022/2555 artikli 22 lõike 1 kohaselt korraldatud kriitilise tähtsusega tarneahelate turvariskide koordineeritud hindamise tulemusi.“;

4) paragrahvi 5 lõiget 4 muudetakse ja sõnastatakse järgmiselt:
„(4) Käesolevas jaos ette nähtud dokumentatsioonid võib koostada muu õigusakti alusel koostatava dokumendi osana.“;

5) määrust täiendatakse normitehnilise märkusega järgmiselt:
„Euroopa Parlamendi ja nõukogu direktiiv (EL) 2022/2555, mis käsitleb meetmeid, millega tagada küberturvalisuse ühtlaselt kõrge tase kogu liidus, ja millega muudetakse määrust (EL) nr 910/2014 ja direktiivi (EL) 2018/1972 ning tunnistatakse kehtetuks direktiiv (EL) 2016/1148 (küberturvalisuse 2. direktiiv) (ELT L 333, 27.12.2022, lk 80–152).“.

§ 3. Vabariigi Valitsuse 3. jaanuari 2024. a määruse nr 1 „Võrgu- ja infosüsteemi turvameetmete nõuded ja nende kohaldamise ulatus pilvteenuse kasutamisel” § 1 lõike 1 punktis 1 asendatakse lauseosa „kohaliku omavalitsuse üksus või küberturvalisuse seaduse § 3 lõike 4 punktides 12 ja 13 nimetatud asutus või isik“ lauseosaga „valitsusasutus, valitsusasutuse hallatava riigiasutus või kohaliku tasandi avaliku halduse üksus“.

§ 4. Määrus jõustub 1. jaanuaril 2026. a.

Kristen Michal
peaminister

Liisa-Ly Pakosta
justiits- ja digiminister

Keit Kasemets
riigisekretär

KAVAND

ENERGEETIKA- JA KESKKONNAMINISTER
MÄÄRUS

Majandus- ja taristuministri 28.06.2018 määruse nr 37 "Elutähtsa teenuse kirjeldus ja toimepidevuse nõuded elektriga varustamisel" muutmine

Määrus kehtestatakse hädaolukorra seaduse § 37 lõike 2 alusel.

Majandus- ja taristuministri 28.06.2018 määruses nr 37 „Elutähtsa teenuse kirjeldus ja toimepidevuse nõuded elektriga varustamisel“ tehakse järgmised muudatused:

1) paragrahvi § 4 lõike 2 punkti 3 täiendatakse pärast sõna „seaduses“ lauseosaga „või asjakohasel juhul Euroopa Komisjoni delegeeritud määruses (EL) 2024/1366, millega täiendatakse Euroopa Parlamendi ja nõukogu määrust (EL) 2019/943 ning kehtestatakse võrgueeskiri piiriüleste elektrivoogude küberturvalisust käsitlevate sektoripõhiste normide kohta,“;

2) määrust täiendatakse normitehnilise märkusega järgmises sõnastuses:
„Komisjoni delegeeritud määrus (EL) 2024/1366, millega täiendatakse Euroopa Parlamendi ja nõukogu määrust (EL) 2019/943 ning kehtestatakse võrgueeskiri piiriüleste elektrivoogude küberturvalisust käsitlevate sektoripõhiste normide kohta (ELT L, 2024/1366, 24.05.2024).“.

Andres Sutt
minister

Marten Kokk
kantsler

KAVAND

JUSTIITS- JA DIGIMINISTER
MÄÄRUS

Majandus- ja infotehnoloogiaministri 17. oktoobri 2023 määruse nr 53 „Küberintsidentide registri põhimäärus“ muutmine

Määrus kehtestatakse küberturvalisuse seaduse § 13 lõike 3 alusel.

§ 1. Majandus- ja infotehnoloogiaministri 17. oktoobri 2023 määruses nr 53 „Küberintsidentide registri põhimäärus“ tehakse järgmised muudatused:
1) paragrahvi 2 muudetakse ja sõnastatakse järgmiselt:
„Registri eesmärk on pidada küberintsidentide, küberohtude ja turvahaavatavuste üle arvestust ning analüüsida registrisse esitatud teavet küberintsidentide, küberohtude ja turvahaavatavuste ennetamiseks või lahendamiseks, ohuteadete edastamiseks ning järelevalvetoimingute tegemiseks.“;

2) paragrahvi 5 lõike 1 punkti 1 ja lõike 2 punkti 1 täiendatakse pärast sõna „küberintsidendist“ lauseosaga „, küberohust või turvahaavatavusest“;

3) paragrahvi 5 lõike 1 punkti 1 ja punkti 8 täiendatakse pärast sõna „küberintsidendi“ lauseosaga „, küberohu või turvahaavatavuse“;

4) paragrahvi 5 lõike 1 punkti 4 ja punkti 8 täiendatakse pärast sõna „küberintsident“ lauseosaga „, küberoht või turvahaavatavus“;

5) paragrahvi 5 lõike 2 punkti 2 täiendatakse pärast sõna „küberintsidenti“ lauseosaga „, küberohtu või turvahaavatavust“;

6) paragrahvi 5 lõike 2 punkt 3 muudetakse ja sõnastatakse järgmiselt:
„3) küberintsidendist, küberohust ja turvahaavatavusest teavitamise kohustuseta isik, kes teavitas küberintsidendist, küberohust või turvahaavatavusest vastutavat töötlejat.“;

7) paragrahv 6 muudetakse ja sõnastatakse järgmiselt:
„**§ 6. Andmeandja**
Andmeandjaks on:
1) teenuseosutaja;
2) muu isik kui teenuseosutaja.“;

8) paragrahvi 7 lõige 3 tunnistatakse kehtetuks;

9) paragrahv 10 muudetakse ja sõnastatakse järgmiselt:
„**§ 10. Registriandmete ja registritoimingute säilitamise tingimused**
(1) Seaduses sätestatud registriandmete ja registritoimingute säilitamise tähtaja saabumisel need kustutatakse.
(2) Andmed, mis on registrisse kantud, kuid ei ole vajalik esitatud küberintsidendi, küberohu või turvahaavatavuse analüüsimiseks, võib kustutada enne seaduses sätestatud tähtaja saabumist.“;

10) määrust täiendatakse normitehnilise märkusega järgmiselt:
„Euroopa Parlamendi ja nõukogu direktiiv (EL) 2022/2555, mis käsitleb meetmeid, millega tagada küberturvalisuse ühtlaselt kõrge tase kogu liidus, ja millega muudetakse määrust (EL) nr 910/2014 ja direktiivi (EL) 2018/1972 ning tunnistatakse kehtetuks direktiiv (EL) 2016/1148 (küberturvalisuse 2. direktiiv) (ELT L 333, 27.12.2022, lk 80–152).“.

§ 2. Määrus jõustub 1. jaanuaril 2026. a.

Liisa-Ly Pakosta
minister

Tiina Uudeberg
kantsler

KAVAND

JUSTIITS- JA DIGIMINISTER
MÄÄRUS

Majandus- ja kommunikatsiooniministri 25. aprilli 2011 määruse nr 28 „Riigi Infosüsteemi Ameti põhimäärus“ muutmine

Määrus kehtestatakse Vabariigi Valitsuse seaduse § 42 lõike 1 alusel.

§ 1. Majandus- ja kommunikatsiooniministri 25.04.2011 määruses nr 28 "Riigi Infosüsteemi Ameti põhimäärus" tehakse järgmised muudatused:

1) paragrahvi 8 lõike 4 punkti 3 muudetakse ja sõnastatakse järgmiselt:
„3) täidab küberturvalisuse seaduse § 5 tähenduses pädeva asutus, ühtse kontaktpunkti, ulatuslike küberintsidentide ja kriiside ohjamise eest vastutava pädeva asutuse, küberintsidentide käsitlemise üksuse ja turvahaavatavuse koordineeritult avaldamise koordinaatori ülesandeid ning koordineerib küberintsidentide käsitlemist;“;

2) paragrahvi 8 lõiget 4 täiendatakse punktiga 3^1 järgmises sõnastuses:
„3^1) osaleb vastavalt pädevusele Euroopa Parlamendi ja nõukogu direktiivi (EL) 2022/2555, mis käsitleb meetmeid, millega tagada küberturvalisuse ühtlaselt kõrge tase kogu liidus, ja millega muudetakse määrust (EL) nr 910/2014 ja direktiivi (EL) 2018/1972 ning tunnistatakse kehtetuks direktiiv (EL) 2016/1148 (küberturvalisuse 2. direktiiv) (ELT L 333, 27.12.2022, lk 80–152), artiklis 14 nimetatud koostöörühma tegevuses, artiklis 16 nimetatud Euroopa küberkriisiga tegelevate kontaktasutuste võrgustikus ning küberturvalisuse seaduse §-s 5 nimetatud küberintsidentide käsitlemise riiklike üksuste võrgustiku töös“;

3) paragrahvi 13 lõike 1 punkti 1 täiendatakse pärast sõna „täitmine“, lauseosaga „küberintsidentide käsitlemise üksuses“;

4) paragrahvi 13 täiendatakse lõigetega 1^1 – 1^5 järgmises sõnastuses:
„(1^1) Küberintsidentide käsitlemise üksus peab:
1) tegelema oma ülesannete piires vähemalt Euroopa Parlamendi ja nõukogu direktiivi (EL) 2022/2555 I ja II lisas osutatud sektoreid, allsektoreid või viidatud liiki üksusi ja vastutama küberintsidentide käsitlemise eest kindla menetluse kohaselt;
2) tagama oma sidekanalite laialdase kättesaadavuse, vältides nõrku lülisid, ja kasutama mitmesuguseid vahendeid, mis võimaldavad tal teistega ja teistel temaga igal ajal ühendust võtta;
3) määrama kindlaks sidekanalid ning tegema need oma sihtrühmadele ja koostööpartneritele teatavaks;
4) tagama, et tema ametiruumid ja tööd toetavad infosüsteemid asuvad turvalises kohas;
5) tagama, et tal on olemas päringute haldamiseks ja suunamiseks sobiv infosüsteem, mis võimaldab ka tööde tõhusat üleandmist;
6) tagama oma tegevuse konfidentsiaalsuse ja usaldusväärsuse;
7) tagama oma teenuste pideva kättesaadavuse eesmärgil piisava arvu töötajate ja ametnike olemasolu;
8) tagama oma töötajatele ja ametnikele asjakohase väljaõppe;
9) tagama oma teenuste toimepidevuse eesmärgil varusüsteemide ja -tööruumide olemasolu.

(1^2) Küberintsidentide käsitlemise üksusel on järgmised ülesanded:
1) osaleb küberturvalisuse seaduses sätestatud vastastikuses hindamises;
2) teeb koostööd teiste küberintsidentide käsitlemise üksustega;
3) võib teha koostööd kolmandate riikide küberintsidentide käsitlemise riiklike üksustega või samaväärsete kolmandate riikide asutustega, eelkõige küberturvalisuse küsimustes abi andmiseks;
4) teeb koostööd teenuseosutajate sektoripõhiste või -vaheliste kogukondadega, sealhulgas vahetades vajaduse korral nendega teavet, arvestades küberturvalisuse seaduses küberturvalisusalase teabevahetuse kokkuleppe kohta sätestatud nõudeid;
5) võib osaleda rahvusvahelistes koostöövõrgustikes;
6) korraldab küberohtude, turvahaavatavuste ja küberintsidentide seiret ning analüüsi riiklikul tasandil;
7) taotluse korral osutab asjaomastele teenuseosutajatele abi nende võrgu- ja infosüsteemide reaalajas või reaalajalähedase seirega;
8) tagab küberohtude, turvahaavatavuste ja küberintsidentide kohta varajaste hoiatuste, hoiatuste ja teadete edastamise ning teabe levitamise asjaomastele teenuseosutajatele, pädevatele asutustele ja muudele asjaomastele sidusrühmadele, võimaluse korral reaalajalähedaselt;
9) lahendab küberintsidente ja asjakohasel juhul abistab asjaomaseid teenuseosutajaid;
10) kogub ja analüüsib digitaalkriminalistika andmeid, analüüsib järjepidevalt riske ja küberintsidente, ning tagab teadlikkuse küberturvalisuse olukorrast;
11) kontrollib potentsiaalselt olulise mõjuga turvahaavatavuste kindlakstegemiseks ennetavalt teenuseosutaja taotlusel teenuseosutaja võrgu- ja infosüsteemi;
12) osaleb küberintsidentide käsitlemise riiklike üksuste võrgustiku töös ja osutab teisele võrgustiku liikmele taotluse korral oma võimekusele ja pädevusele vastavat abi;
13) täidab turvahaavatavuse koordineeritult avaldamise koordinaatori ülesandeid;
14) aitab teenuseosutajatel ja asjaomastel sidusrühmadel kasutusele võtta nendega teabe turvaliseks vahetamiseks mõeldud teabe vahetamise vahendeid;
15) teeb vajaduse korral teenuseosutaja üldkasutatava võrgu- ja infosüsteemi ennetavat välist kontrolli, kui selle eesmärk on tuvastada nõrk või ebaturvaliselt konfigureeritud süsteem ja teavitada asjaomast teenuseosutajat, ning selline kontrollimine ei tohi avaldada negatiivset mõju teenuseosutaja osutatava teenuse toimimisele;
16) loob koostöösuhteid asjaomaste erasektori sidusrühmadega.
(1^3) Küberintsidentide käsitlemise üksus võib lõike 1^2 punktides 6–14 sätestatud ülesandeid riski- või ohuprognoosipõhise lähenemisviisi alusel prioriseerida.
(1^4) Lõike 1^2 punktis 16 nimetatud koostöö hõlbustamiseks toetab küberintsidentide käsitlemise üksus ühtsete või standardsete tavade, liigitamissüsteemide ja taksonoomiate kasutuselevõttu seoses küberintsidentide käsitlemise menetluste, kriisiohje ja turvahaavatavuste koordineeritud avaldamisega.
(1^5) Küberintsidentide käsitlemise üksus teeb turvahaavatavuse koordineeritult avaldamise koordinaatori ülesandeid täites järgmist:
1) tegutseb usaldusväärse vahendajana, hõlbustades vajaduse korral turvahaavatavusest teavitava füüsilise või juriidilise isiku ja potentsiaalse turvahaavatavusega IKT-toodete tootja või IKT-teenuste osutaja vahelist suhtlust, tegutsedes ükskõik kumma poole taotlusel;
2) teeb kindlaks teavitatud potentsiaalse turvahaavatavuse või turvahaavatavusega seotud üksuse ja võtab temaga ühendust;
3) abistab potentsiaalsest turvahaavatavusest ja turvahaavatavusest teavitavat füüsilist või juriidilist isikut;
4) peab läbirääkimisi turvahaavatavusest avalikkuse teavitamise tähtaja üle;
5) haldab mitut teenuseosutajat mõjutavaid turvahaavatavusi;

6) tagab, et teatatud turvahaavatavusega seoses võetakse hoolikalt järelmeetmeid;
7) tagab potentsiaalsest turvahaavatavusest või turvahaavatavusest teatava füüsilise või juriidilise isiku anonüümsuse;
8) teeb teise Euroopa Liidu liikmesriigi poolt turvahaavatavuste koordineeritult avaldamise koordinaatori ülesandeid täitma määratud küberintsidentide käsitlemise riikliku üksusega küberintsidentide käsitlemise riiklike üksuste võrgustikus koostööd, kui teatatud turvahaavatavus võib oluliselt mõjutada teenuseosutajaid rohkem kui ühes Euroopa Liidu liikmesriigis.“;

5) määrust täiendatakse normitehnilise märkusega järgmiselt:
„Euroopa Parlamendi ja nõukogu direktiiv (EL) 2022/2555, mis käsitleb meetmeid, millega tagada küberturvalisuse ühtlaselt kõrge tase kogu liidus, ja millega muudetakse määrust (EL) nr 910/2014 ja direktiivi (EL) 2018/1972 ning tunnistatakse kehtetuks direktiiv (EL) 2016/1148 (küberturvalisuse 2. direktiiv) (ELT L 333, 27.12.2022, lk 80–152).“.

§ 2. Määrus jõustub 1. jaanuaril 2026. a.

Liisa-Ly Pakosta
minister

Tiina Uudeberg
kantsler

KAVAND

JUSTIITS- JA DIGIMINISTER
MÄÄRUS

Riikliku küberturvalisuse strateegia koostamise ulatus, tingimused ja elluviimise kord[1]

Määrus kehtestatakse küberturvalisuse seaduse § 5 lõike 2 alusel.

§ 1. Kohaldamisala
(1) Määrust kohaldatakse Euroopa Parlamendi ja nõukogu direktiiv (EL) 2022/2555, mis käsitleb meetmeid, millega tagada küberturvalisuse ühtlaselt kõrge tase kogu liidus, ja millega muudetakse määrust (EL) nr 910/2014 ja direktiivi (EL) 2018/1972 ning tunnistatakse kehtetuks direktiiv (EL) 2016/1148 (küberturvalisuse 2. direktiiv) (ELT L 333, 27.12.2022, lk 80–152), artiklis 7 sätestatud riikliku küberturvalisuse strateegia (edaspidi *strateegia*) koostamisel.
(2) Strateegias määratakse kindlaks strateegilised eesmärgid, nende eesmärkide saavutamiseks vajalikud ressursid ning asjakohased poliitilised ja regulatiivsed meetmed, et saavutada ja säilitada kõrgel tasemel küberturvalisus.
(3) Määruses sätestatakse strateegia ulatus, tingimused ja elluviimise kord ning asjaomaste poliitikameetmete loetelu.

§ 2. Strateegia põhisisu
Strateegia peab sisaldama järgmist:
1) strateegia eesmärgid ja prioriteedid, mis hõlmavad eelkõige Euroopa Parlamendi ja nõukogu direktiiv (EL) 2022/2555 I ja II lisas osutatud sektoreid;
2) juhtimisraamistik punktis 1 osutatud eesmärkide ja prioriteetide saavutamiseks, sealhulgas §-s 3 osutatud poliitikameetmed;
3) juhtimisraamistik, milles selgitatakse asjaomaste sidusrühmade rolli ja kohustusi riiklikul tasandil, mis toetavad Riigi Infosüsteemi Ameti, julgeolekuasutuste ja muude küberturvalisuse valdkonnaga seotud asutuste vahelist koostööd ja koordineerimist riiklikul tasandil, samuti nende asutuste ja valdkondlike liidu õigusaktide kohaste pädevate asutuste vahelist koordineerimist ja koostööd;
4) mehhanism asjakohaste ressursside kindlaks tegemiseks ja üleriigilise riskihinnangu koostamine;
5) küberintsidentideks valmisoleku ja neile reageerimise meetmete ning seotud taastemeetmete, sealhulgas avaliku ja erasektori koostöö kirjeldus;
6) strateegia rakendamisse kaasatavate asutuste ja sidusrühmade loetelu;
7) poliitikaraamistik küberturvalisuse seaduses sätestatud pädevate asutuste, elutähtsat teenust korraldava asutuse või tema poolt hädaolukorra seaduse § 37 lõike 5 alusel määratud asutuse, Päästeameti ja Riigikantselei vahelise tegevuse tõhusaks koordineerimiseks küberriskide, küberohtude ja küberintsidentide ning asjakohasel juhul muude kui küberriskide, küberohtude ja küberintsidentide alase teabe jagamise ning järelevalveülesannete täitmise eesmärgil;
8) kava, sealhulgas vajalikud meetmed elanike küberturvalisuse alase teadlikkuse üldise taseme suurendamiseks.

§ 3. Strateegia poliitikameetmed
Strateegia osaks on poliitikameetmed:
1) mis käsitlevad üksuste teenuste osutamiseks kasutatavate IKT-toodete ja IKT-teenuste tarneahela küberturvalisust;

2) mis käsitlevad IKT-toodete ja IKT-teenuste küberturvalisusega seotud nõuete ja vastavate spetsifikatsioonide lisamist riigihankemenetlusse, sealhulgas seoses küberturvalisuse sertifitseerimise, krüpteerimisnõuete ning avatud lähtekoodiga küberturvalisuse toodete kasutamisega;
3) turvahaavatavuste haldamiseks, mis hõlmab turvahaavatavuste koordineeritud avaldamise edendamist ja hõlbustamist;
4) mis on seotud avatud interneti avaliku tuuma üldise kättesaadavuse, usaldusväärsuse ja konfidentsiaalsuse säilitamisega, sealhulgas vajaduse korral merealuste sidekaablite küberturvalisusega;
5) mis edendavad selliste asjakohaste kõrgetasemeliste tehnoloogiate väljatöötamist ja integreerimist, mille eesmärk on rakendada ajakohaseid küberturvalisuse riskijuhtimismeetmeid;
6) mille abil edendatakse ja arendatakse küberturvalisuse alast haridust ja koolitust, küberturvalisuse alaseid oskusi, teadlikkust, teadus- ja arendusalgatusi ning suuniseid heade küberhügieenitavade ja küberkontrolli meetmete kohta elanikele, sidusrühmadele ja üksustele;
7) millega edendatakse akadeemilisi ja teadusasutusi küberturvalisuse vahendite ja turvalise võrgutaristu väljatöötamisel, täiustamisel ja kasutuselevõtmise edendamisel;
8) asjakohane menetluskord ja sobivad teabevahetuslahendused, millega toetatakse vabatahtlikku küberturvalisuse alase teabe vahetamist üksuste vahel kooskõlas õigusaktidega;
9) mis tugevdavad väikeste ja keskmise suurusega ettevõtjate, eelkõige nende, kes on küberturvalisuse seaduse kohaldamisalast välja jäetud, küberkerksust ja küberhügieeni lähtetaset, pakkudes nende erivajaduste rahuldamiseks kergesti kättesaadavaid suuniseid ja abi;
10) mis edendavad aktiivset küberkaitset.

§ 4. Strateegiast teavitamine
(1) Justiits- ja Digiministeerium teavitab Euroopa Komisjoni strateegia vastu võtmisest kolme kuu jooksul pärast selle vastu võtmist.
(2) Lõike 1 alusel edastatavast teabest võib jätta välja teabe, mis on seotud riigi julgeolekuga.

§ 5. Strateegia hindamine ja uuendamine
Strateegiat hinnatakse peamiste tulemusnäitajate põhjal korrapäraselt ja vähemalt iga viie aasta tagant ning vajadusel ajakohastatakse seda.

§ 6. Määrus jõustub 1. jaanuaril. 2026. a.

[1] Euroopa Parlamendi ja nõukogu direktiiv (EL) 2022/2555, mis käsitleb meetmeid, millega tagada küberturvalisuse ühtlaselt kõrge tase kogu liidus, ja millega muudetakse määrust (EL) nr 910/2014 ja direktiivi (EL) 2018/1972 ning tunnistatakse kehtetuks direktiiv (EL) 2016/1148 (küberturvalisuse 2. direktiiv) (ELT L 333, 27.12.2022, lk 80–152).

Liisa-Ly Pakosta
minister

Tiina Uudeberg
kantsler

KAVAND

JUSTIITS- JA DIGIMINISTER
MÄÄRUS

Sihipärase turvaauditi korraldamise täpsemad tingimused ja kord[1]

Määrus kehtestatakse küberturvalisuse seaduse § 16 lõike 1^2 ja § 17 lõike 1^2 alusel.

§ 1. Kohaldamisala
(1) Määrust kohaldatakse, kui toimub küberturvalisuse seaduse § 16 lõike 1^1 punkti 2 ja § 17 lõike 1^1 punkti 2 kohane sihipärane turvaaudit riiklikus või haldusjärelevalvemenetluses (edaspidi *sihipärane turvaaudit*).
(2) Määrus täpsustab sihipärase turvaauditi korraldamise täpsemad tingimused ja korra, sealhulgas loetelu olukordadest, mille puhul Riigi Infosüsteemi Amet hüvitab teenuseosutajale sihipärase turvaauditi kulu ja kulu hüvitamise korra.

§ 2. Sihipärase turvaauditi korraldamise tingimused ja kord
(1) Sihipärasele turvaauditile kohalduvad järgmised tingimused:
1) seda võib Riigi Infosüsteemi Amet teha üliolulise üksuse suhtes korrapäraselt;
2) seda teeb sõltumatu organisatsioon või Riigi Infosüsteemi Amet;
3) selle tulemused tehakse kättesaadavaks Riigi Infosüsteemi Ametile;
4) selle kulud kannab auditeeritav teenuseosutaja, välja arvatud põhjendatud juhtudel, kui Riigi Infosüsteemi Amet otsustab teisiti.
(2) Riigi Infosüsteemi Amet viib läbi hanke riigihangete seaduses korras sihipärases turvaauditis kasutatava sõltumatu organisatsiooni leidmiseks.

§ 3. Teenuseosutaja kulude hüvitamise olukorrad
Põhjendatud juhud, kui Riigi Infosüsteemi Amet hüvitab teenuseosutajale sihipärase turvaauditi kulud:
1)
2)
3)

§ 4. Teenuseosutaja kulude hüvitamise tingimused ja kord

§ 5. Määrus jõustub 1. jaanuaril. 2026. a.

[1] Euroopa Parlamendi ja nõukogu direktiiv (EL) 2022/2555, mis käsitleb meetmeid, millega tagada küberturvalisuse ühtlaselt kõrge tase kogu liidus, ja millega muudetakse määrust (EL) nr 910/2014 ja direktiivi (EL) 2018/1972 ning tunnistatakse kehtetuks direktiiv (EL) 2016/1148 (küberturvalisuse 2. direktiiv) (ELT L 333, 27.12.2022, lk 80–152).

Liisa-Ly Pakosta
minister

Tiina Uudeberg
kantsler

KAVAND

JUSTIITS- JA DIGIMINISTER
MÄÄRUS

Vastastikuse hindamise täpsemad tingimused[1]

Määrus kehtestatakse küberturvalisuse seaduse § 17^6 lõike 3 alusel.

§ 1. Kohaldamisala
(1) Määrust kohaldatakse, kui Eesti Vabariik osaleb või Eesti Vabariigi suhtes viiakse läbi Euroopa Parlamendi ja nõukogu direktiiv (EL) 2022/2555, mis käsitleb meetmeid, millega tagada küberturvalisuse ühtlaselt kõrge tase kogu liidus, ja millega muudetakse määrust (EL) nr 910/2014 ja direktiivi (EL) 2018/1972 ning tunnistatakse kehtetuks direktiiv (EL) 2016/1148 (küberturvalisuse 2. direktiiv) (ELT L 333, 27.12.2022, lk 80–152), artiklis 19 sätestatud vastastikust hindamist (edaspidi *vastastikune hindamine*).
(2) Määrus täpsustab vastastiku hindamises osalemise täpsemaid tingimusi, sealhulgas vastastikuse hindamise läbiviimise korralduse nõuded, selles osalevate asutuste ülesanded ja vastastikuses hindamises osalevad isikud.

§ 2. Vastastikuse hindamise metoodika, korralduslikud aspektid ja tegevusjuhendid
(1) Vastastikuses hindamises osalemise korral lähtutakse Euroopa Parlamendi ja nõukogu direktiivi (EL) 2022/2555 artikli 19 lõigetes 1 ja 6 nimetatud vastastikuse hindamise metoodikast, korralduslikest aspektidest ning tegevusjuhenditest, kui need on välja töötatud.
(2) Vastastikuse hindamise käigus:
1) võidakse korraldada kohapealseid või virtuaalseid kohtumisi ja teabevahetust väljaspool hinnatavat tegevuskohta;
2) saadavat teavet kasutatakse üksnes vastastikuse hindamise eesmärgil;
3) hinnatud aspekte kõnealuses riigis kahe aasta jooksul pärast vastastikuse hindamise lõppemist enam uuesti vastastikku ei hinnata, välja arvatud juhul, kui seda taotleb Eesti Vabariik või nii lepitakse kokku pärast Euroopa Parlamendi ja nõukogu direktiivi (EL) 2022/2555 artiklis 14 nimetatud koostöörühma (edaspidi *koostöörühm*) ettepanekut;
4) koostavad osalevad küberturvalisuse eksperdid aruandeid vastastikuse hindamise tulemuste ja järelduste kohta;
5) koostatud aruanded sisaldavad soovitusi vastastikku hinnatavate aspektide parandamiseks.

§ 3. Vastastikuses hindamises osalevad isikud
Vastastikust hindamises osalevad küberturvalisuse valdkonna eksperdid, arvestades § 2 lõikes 1 viidatud metoodikas sätestatud kriteeriume.

§ 4. Vastastikuses hindamises osalevad asutused ja ülesanded
(1) Justiits- ja Digiministeerium või tema volitatud asutus:
1) määrab kindlaks teise Euroopa Liidu liikmesriigi suhtes tehtavas vastastikuses hindamises Eesti Vabariigist osalevad küberturvalisuse valdkonna eksperdid;
2) teavitab vastastikuses hindamises osalevaid Euroopa Liidu liikmesriike, koostöörühma, Euroopa Komisjoni ja Euroopa Liidu Küberturvalisuse Ametit käesoleva lõike punkti 1 alusel määratud ekspertidega seotud huvide konflikti ohust enne vastastikuse hindamise alustamist;
3) võib põhjendatud juhul esitada vastuväite Eesti Vabariiki hindava teise Euroopa Liidu liikmesriigi küberturvalisuse valdkonna eksperdi määramise kohta asjakohasele Euroopa Liidu liikmesriigile;

4) määrab kindlaks vastastikuse hindamise käigus hinnatavate aspektide sisu ja ulatuse, arvestades Euroopa Parlamendi ja nõukogu direktiivi (EL) 2022/2555 artikli 19 lõigetes 1 ja 3 sätestatud nõudeid, ning teavitab nendest vastastikuses hindamises osalevatele Euroopa Liidu liikmesriikidele enne vastastikuse hindamise alustamist, kui vastastikuse hindamise käigus hinnatakse Eesti Vabariiki;
5) võib enne vastastikuse hindamise algust koordineerida vastastikuse hindamise käigus Eesti Vabariigi puhul hinnatavate aspektide enesehindamist, arvestades Euroopa Parlamendi ja nõukogu direktiivi (EL) 2022/2555 artikli 19 lõike 5 alusel kehtestatud metoodikat, ning esitab enesehindamise tulemused Eesti Vabariiki hindavatele Euroopa Liidu liikmesriikide küberturvalisuse valdkonna ekspertidele;
6) edastab Eesti Vabariiki hindavatele Euroopa Liidu liikmesriikide määratud küberturvalisuse valdkonna ekspertidele hindamiseks vajaliku teabe;
7) võib esitada § 5 punktis 4 nimetatud taotluse;
8) võib koondada ja esitada märkusi Eesti Vabariiki käsitleva aruande kavandi kohta;
9) võib vajaduse korral esitada koostöörühmale ning Euroopa Parlamendi ja nõukogu direktiivi (EL) 2022/2555 artiklis 16 nimetatud Euroopa küberkriisiga tegelevate kontaktasutuste võrgustikule aruande Eesti Vabariigi suhtes tehtud vastastikuse hindamise kohta;
10) võib teha Eesti Vabariigi kohta koostatud vastastikuse hindamise aruande või selle toimetatud versiooni üldsusele kättesaadavaks.
(2) Lõike 1 punktis 6 nimetatud teabe edastamisel arvestatakse:
1) vastastikuse hindamise käigus hinnatavaid aspekte ja hindamise ulatust;
2) juurdepääsupiiranguga teabe ja salastatud teabe kaitset;
3) Eesti Vabariigi, sealhulgas julgeolekuhuve ja
4) riigi julgeoleku suhtes kehtivaid õigusakte.

§ 5. Vastastikuse hindamise
Vastastikuse hindamise käigus:
1) võidakse korraldada kohapealseid või virtuaalseid kohtumisi ja teabevahetust väljaspool hinnatavat tegevuskohta;
2) saadavat teavet kasutatakse üksnes vastastikuse hindamise eesmärgil;
3) hoiavad osalevad küberturvalisuse valdkonna eksperdid kolmandate isikute eest saladuses neile vastastikuse hindamise käigus teatavaks saanud teavet, kui seadus ei sätesta samaväärset saladuses hoidmise kohustust;
4) hinnatud aspekte kõnealuses riigis kahe aasta jooksul pärast vastastikuse hindamise lõppemist enam uuesti vastastikku ei hinnata, välja arvatud juhul, kui seda taotleb Eesti Vabariik või nii lepitakse kokku pärast koostöörühma ettepanekut;
5) koostavad osalevad küberturvalisuse eksperdid aruandeid vastastikuse hindamise tulemuste ja järelduste kohta;
6) koostatud aruanded sisaldavad soovitusi vastastikku hinnatavate aspektide parandamiseks.

§ 6. Määrus jõustub 1. jaanuaril. 2026. a.

[1] Euroopa Parlamendi ja nõukogu direktiiv (EL) 2022/2555, mis käsitleb meetmeid, millega tagada küberturvalisuse ühtlaselt kõrge tase kogu liidus, ja millega muudetakse määrust (EL) nr 910/2014 ja direktiivi (EL) 2018/1972 ning tunnistatakse kehtetuks direktiiv (EL) 2016/1148 (küberturvalisuse 2. direktiiv) (ELT L 333, 27.12.2022, lk 80–152).

Liisa-Ly Pakosta
minister

Tiina Uudeberg
kantsler

KAVAND

JUSTIITS- JA DIGIMINISTER
MÄÄRUS

Küberturvalisuse taseme tõstmise toetuse tingimused ja kord

Määrus kehtestatakse küberturvalisuse seaduse § 28^2 lõike 3 ja riigieelarve seaduse § 53^1 lõike 1 alusel.

Liisa-Ly Pakosta
minister

Tiina Uudeberg
kantsler