

## MINISTRI MÄÄRUS

### Riikliku küberturvalisuse strateegia koostamise ulatus, tingimused ja elluviimise kord<sup>1</sup>

Määrus kehtestatakse küberturvalisuse seaduse § 5 lõike 2 alusel.

#### § 1. Reguleerimisala

(1) Määrusega reguleeritakse 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 7 sätestatud riikliku küberturvalisuse strateegia (edaspidi *strateegia*) koostamist.

(2) Määruses sätestatakse strateegiakoostamise nõuded ja kord ning asjaomaste poliitikameetmete loetelu.

#### § 2. Strateegia põhisisu

(1) Strateegias määratakse kindlaks strateegilised eesmärgid, nende eesmärkide saavutamiseks vajalikud ressursid ning asjakohased poliitilised ja regulatiivsed meetmed, et saavutada ja säilitada kõrge tasemel küberturvalisus.

(2) Strateegia peab sisaldama järgmist:

- 1) strateegia eesmärgid ja prioriteetidid eelkõige Euroopa Parlamendi ja nõukogu direktiivi (EL) 2022/2555 I ja II lisas osutatud sektorite kohta;
- 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 tegevuse koordineerimist riiklikul tasandil ning nimetatud asutuste ja valdkondlike liidu õigusaktide kohaste pädevate asutuste vahelist tegevuse koordineerimist ja koostööd;
- 4) asjakohaste ressursside kindlakstegemise mehhanism ja üleriigiline riskihinnang;
- 5) küberintsidentideks valmisoleku ja neile reageerimise meetmete ning seotud taastemeetmete, sealhulgas avaliku ja erasektori sellealase koostöö kirjeldus;
- 6) strateegia rakendamisse kaasatavate asutuste ja sidusrühmade loetelu;
- 7) poliitikaamistik küberturvalisuse seaduses sätestatud pädevate asutuste, elutähtsa teenuse toimepidevust korraldava asutuse või tema poolt hädaolukorra seaduse § 37 lõike 5 alusel määratud asutuse, Päästeameti ja Riigikantselei vahelise tegevuse tõhusaks koordineerimiseks küberriskide, küberohtude ja küberintsidentide alase ning asjakohasel juhul muu teabe jagamise ning järelevalveülesannete täitmise eesmärgil;
- 8) kava, sealhulgas vajalikud meetmed elanike üldise küberturvalisusalase teadlikkuse parandamiseks.

#### § 3. Strateegia poliitikameetmed

(1) Strateegias määratakse kindlaks 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, muu hulgas turvahaavatavuste koordineeritud avaldamise edendamise ja hõlbustamise teel;

- 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 küberturvalisusalast haridust, koolitust ja teadlikkust, küberturvalisusalaseid oskusi ning teadus- ja arendusalgatusi ning suuniseid heade küberhügieenitavade ja küberkontrolli tagavate meetmete kohta elanikele, sidusrühmadele ja üksustele;
- 7) millega toetatakse akadeemilisi ja teadusasutusi küberturvalisuse vahendite ja turvalise võrgutaristu väljatöötamisel, täiustamisel ja kasutuselevõtmise edendamisel;
- 8) asjakohane menetluskord ja sobivad teabevahetusvahendid, millega toetatakse vabatahtlikku küberturvalisusalase teabe vahetamist üksuste vahel kooskõlas õigusaktidega;
- 9) mis tugevdavad väike- ja keskmise suurusega ettevõtjate, eelkõige küberturvalisuse seaduse kohaldamisalast välja jäetud väike- ja keskmise suurusega ettevõtjate küberkerksust ja baastasemel küberhügieeni, pakkudes nende spetsiifiliste vajaduste rahuldamiseks kergesti kättesaadavaid suuniseid ja abi;
- 10) mis edendavad aktiivset küberkaitset.

(2) Lisaks lõikes 1 nimetatud poliitikameetmetele võib strateegia sisaldada ka muid poliitikameetmeid.

#### **§ 4. Strateegia koostamine nõuded ja teavitamine**

(1) Strateegia viiakse ellu valdkonna arengukava programmiga riigieelarve seaduse § 19 tähenduses ning lähtuvalt valdkonna arengukava ja programmi koostamise, elluviimise, aruandluse, hindamise ja muutmise korrast, kui käesolev määrus ei sätesta teisiti.

(2) Justiits- ja Digiministerium teavitab Euroopa Komisjoni strateegia vastuvõtmisest kolme kuu jooksul pärast selle vastuvõtmist.

(3) Lõike 2 alusel edastatavast teabest võib välja jätta teabe, mis on seotud riigi julgeolekuga.

#### **§ 5. Strateegia hindamine ja uuendamine**

Strateegiat hinnatakse peamiste tulemusnäitajate põhjal regulaarselt ja vähemalt iga viie aasta tagant ning vajaduse korral ajakohastatakse seda.

<sup>1</sup> 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  
justiits- ja digiminister

Tiina Uudeberg  
kantsler