Küberturvalisuse seaduse ja teiste
seaduste muutmise seaduse
eelnõu seletuskirja juurde

Lisa 2

VABARIIGI VALITSUS
MÄÄRUS

Võrgu- ja infosüsteemide küberturvalisuse nõuded

Määrus kehtestatakse küberturvalisuse seaduse § 7 lõike 5 alusel.

1. peatükk
Üldsätted

§ 1. Reguleerimisala

Määrusega kehtestatakse küberturvalisuse seaduse §-s 7 sätestatud kohustuste täitmise ja süsteemide küberturvalisuse tagamiseks:

1) infoturbe halduse nõuded, üldnimetusega Eesti Infoturbestandard;

2) turvameetmete üldnõuded;

3) süsteemide turvameetmete erinõuded ning nende kohaldamise ulatuse.“;

§ 2. Terminid

(1) Andmekogu on andmekogu avaliku teabe seaduse tähenduses.

(2) Infoturve on võrgu- ja infosüsteemile turvameetmete loomise, valimise ja rakendamise protsesside kogum.

(3) Määruses kasutatakse termineid küberturvalisuse seaduse §-s 2 määratud tähenduses.

2. peatükk
Eesti Infoturbestandard

§ 3. Eesti Infoturbestandardi sisu

(1) Teenuse osutaja peab järgima Eesti Infoturbestandardit ning rakendama selle järgimisest tulenevaid turvameetmeid.

(2) Eesti Infoturbestandardi järgimine seisneb Eesti Infoturbestandardi tingimuste täitmises infoturbe halduse käivitamisel, rakendamisel, käigushoidmisel ning täiustamisel ja Eesti Infoturbestandardi tingimuste täitmise auditeerimises.

(3) Eesti Infoturbestandardi kehtestab üleriigilise küberturvalisuse tagamise korraldamise eest vastutav minister määrusega ning selle sisu avaldatakse Eesti Infoturbestandardi portaalis.

(4) Lõikes 1 sätestatud kohustus loetakse täidetuks, kui on täidetud kõik järgmised tingimused:

1) teenuse osutaja rakendatud turvameetmed vastavad rahvusvahelise standardiga ISO/IEC 27001 kehtestatud nõuetele;

2) teenuse osutaja on punktis 1 nimetatud tingimuse täitmise kinnitamiseks esitanud Riigi Infosüsteemi Ametile kehtiva vastavussertifikaadi.

§ 4. Eesti Infoturbestandardi järgimise auditeerimine

(1) Teenuse osutaja peab läbi viima Eesti Infoturbestandardi tingimuste täitmise sõltumatu auditi iga kolme aasta järel. Auditeerimine viiakse läbi vastavalt küberturvalisuse seaduse § 7 lõike 5 ning määruse § 3 lõike 3 alusel kehtestatud Eesti Infoturbestandardi auditeerimisjuhendile.

(2) Teenuse osutaja edastab lõike 1 alusel läbiviidud auditi järeldusotsuse Riigi Infosüsteemi Ametile.

(3) Käesoleva paragrahvi lõikes 1 sätestatud kohustuse loetakse täidetuks, kui on täidetud üks järgnevatest punktidest:

1) teenuse osutaja on täitnud § 3 lõikes 4 olevad tingimused;

2) teenuse osutaja on küberturvalisuse seaduse § 3 lõike 1 punktis 7 nimetatud perearst; või

3) tegemist on valla, linna, osavalla või linnaosa asutuse hallatava asutusega või valitsusasutuse hallatava riigiasutusega ning sellele isikule kohaldatakse küberturvalisuse seaduse §-s 7 sätestatud kohustusi ainult sama seaduse § 3 lõike 4 alusel.

3. peatükk
Turvameetmete nõuded

1. jagu

Turvameetmete üldnõuded

§ 5. Teenuste kaardistuse ja turvameetmete dokumentatsioon

(1) Teenuse osutaja kaardistab ning dokumenteerib enda teenused, teenuste haldamiseks asjakohased süsteemid, riskianalüüsi ja süsteemidele rakendatavad turvameetmed.

(2) Teenuse osutaja ajakohastab riskianalüüsi:

1) viivitamatult pärast olulise mõjuga küberintsidendi toimumist;

2) teenuse osutamiseks kasutatava süsteemi sellist muutust, mis mõjutab süsteemi turvalisust; või

3) hiljemalt kolme aasta möödumisel viimasest ajakohastamisest.

(3) Teenuse osutaja peab lõikes 1 nimetatud dokumentatsiooni säilitama 7 aastat alates selle koostamisest ning tegema vastava taotluse korral selle Riigi Infosüsteemi Ametile kättesaadavaks.

(4) Teenuse osutaja võib lõikes 1 nimetatud dokumentatsiooni koostada muu õigusakti alusel koostatava dokumendi osana.

2. jagu
Turvameetmete erinõuded

1. alljaotis

Andmekogu

§ 6. Turvameetmete nõuete erisused andmekogu pidamisel

(1) Andmekogu vastutav töötleja korraldab andmekogu andmete turvaklassi määramiseks andmete tähtsuse hindamise ning andmete turvalisuse puudumisest tuleneva kahjude hindamise.

(2) Andmekogu andmetele määratud turvaklass ja turbeaste kooskõlastatakse koos andmekogu registreerimiseks või andmekogu andmete ajakohastamiseks ettevalmistatava tehnilise dokumentatsiooniga avaliku teabe seaduse § 43^9 lõike 1 punkti 6 alusel kehtestatud õigusaktis sätestatud korras.

(3) Andmekogu kasutusele võtmise ajaks peavad turvameetmed olema rakendatud.

(4) Andmekogu vastutav töötleja ja andmekogu majutamisel volitatud töötleja juures volitatud töötleja rakendavad andmekogu pidamisega seotud süsteemide turvameetmeid andmekogu turbeastmest lähtuvalt.

§ 7. Andmekogu turbeastme määramine

(1) Turbeaste võib olla kõrge (H), keskmine (M) või madal (L).

(2) Andmekogu turbeaste määratakse lähtuvalt andmete turvaklassist. Kui andmete turvaklassi vähemalt üks osaklass vastab tasemele 3, siis on andmekogu turbeaste kõrge (H). Kui andmete turvaklassi vähemalt üks osaklass vastab tasemele 2, siis on andmekogu turbeaste vähemalt keskmine (M). Muul juhul on andmekogu turbeaste vähemalt madal (L).

§ 8. Andmete turvaklassi määramine

(1) Andmete turvaklass määratakse vastavalt infoturbe eesmärkidele tervikluse, konfidentsiaalsuse ja käideldavuse parameetrite kaudu.

(2) Andmete turvaklass on kombinatsioon andmete käideldavuse (K), tervikluse (T) ja konfidentsiaalsuse (S) turvaosaklasside tasemetest. Andmete turvaklassi tähis moodustatakse osaklasside tähistest nende järjestuses KTS (näiteks K2T3S1).

(3) Andmete terviklus on andmete õigsuse, täielikkuse ja ajakohasuse tagatus ning päritolu autentsus ja volitamatute muutuste puudumine.

(4) Andmete konfidentsiaalsus on andmete kättesaadavus ainult selleks volitatud isikule või tehnilisele vahendile.

(5) Andmete käideldavus on eelnevalt kokku lepitud vajalikul ja nõutaval tööajal kasutamiskõlblike andmete õigeaegne ja hõlbus kättesaadavus (st vajalikul ja nõutaval ajahetkel ja vajaliku ning nõutava aja jooksul) selleks volitatud isikule või tehnilisele vahendile.

§ 9. Andmete turvaosaklasside määramine

(1) Andmete turvaosaklass on andmete tähtsusest tulenev infoturbe eesmärgi saavutamise nõutav tase.

(2) Andmekogu vastutav töötleja määrab andmete käideldavuse, tervikluse ja konfidentsiaalsuse turvaosaklasside tasemed vastavalt käesolevas paragrahvis sätestatud skaalale. Turvaosaklasside taseme määramisel lähtub andmekogu vastutav töötleja järgnevast:

1) andmetega seotud nõuded õigusaktidest ja lepingulistest kohustustest tulenevalt;

2) andmetega seotud nõuded pakutavate teenuste iseloomust tulenevalt;

3) küberintsidentidest tekkivate kahjude olulisus.

(3) Andmete käideldavuse alusel määratakse turvaosaklass järgmisest skaalast:

1) K0 – töökindlus – pole oluline; jõudlus – pole oluline;

2) K1 – töökindlus – 90% (lubatud summaarne seisak nädalas ~ ööpäev); lubatav nõutava reaktsiooniaja kasv tippkoormusel – tunnid (1÷10);

3) K2 – töökindlus – 99% (lubatud summaarne seisak nädalas ~ 2 tundi); lubatav nõutava reaktsiooniaja kasv tippkoormusel – minutid (1÷10);

4) K3 – töökindlus – 99,9% (lubatud summaarne seisak nädalas ~ 10 minutit); lubatav nõutava reaktsiooniaja kasv tippkoormusel – sekundid (1÷10).

(4) Andmete tervikluse alusel määratakse turvaosaklass järgmisest skaalast:

1) T0 – info allikas, muutmise ega hävitamise tuvastatavus ei ole olulised; info õigsuse, täielikkuse ja ajakohasuse kontroll pole vajalik;

2) T1 – info allikas, selle muutmise ja hävitamise fakt peavad olema tuvastatavad; info õigsuse, täielikkuse ja ajakohasuse kontroll erijuhtudel ja vastavalt vajadusele;

3) T2 – info allikas, selle muutmise ja hävitamise fakt peavad olema tuvastatavad; vajalik on info õigsuse, täielikkuse ja ajakohasuse perioodiline kontroll;

4) T3 – info allikas, selle muutmise ja hävitamise faktil peab olema tõestusväärtus; vajalik on info õigsuse, täielikkuse ja ajakohasuse kontroll reaalajas.

(5) Andmete konfidentsiaalsuse alusel määratakse turvaosaklass järgmisest skaalast:

1) S0 – avalik info: juurdepääsu teabele ei piirata (st lugemisõigus on kõigil huvitatutel, muutmise õigus on määratud tervikluse nõuetega);

2) S1 – info asutusesiseseks kasutamiseks: juurdepääs teabele on lubatav juurdepääsu taotleva isiku teadmisvajaduse korral;

3) S2 – salajane info: info kasutamine on lubatud ainult teatud kindlatele kasutajate gruppidele, juurdepääs teabele on lubatav juurdepääsu taotleva isiku teadmisvajaduse korral;

4) S3 – ülisalajane info: info kasutamine on lubatud ainult teatud kindlatele kasutajatele, juurdepääs teabele on lubatav juurdepääsu taotleva isiku teadmisvajaduse korral.

§ 10. Turvameetmete rakendamine andmekogu turbeastmest lähtuvalt

(1) Paragrahvi 6 lõikes 4 sätestatud kohustuse täitmiseks peab andmekogu vastutav või asjakohasel juhul andmekogu majutav volitatud töötleja Eesti Infoturbestandardi järgimisel lähtuma kaitsealast, mis hõlmab vähemalt kõiki andmekogu pidamisega seotud süsteeme, määrama kõikidele andmekogu pidamisega seotud süsteemidele ja teenustele vähemalt andmekogu turbeastmele vastava kaitsetarbe ning rakendama Eesti Infoturbestandardi etalonturbe standardturve turbeviisi.

(2) Turbeastmele kõrge (H) vastav Eesti Infoturbestandardi kaitsetarve on väga suur (VS), turbeastmele keskmine (M) vastav Eesti Infoturbestandardi kaitsetarve on suur (S) ning turbeastmele madal (L) vastav Eesti Infoturbestandardi kaitsetarve on normaalne (N).

(3) Lõikes 1 sätestatud kohustus loetakse täidetuks, kui andmekogu vastutav või majutamiseks volitatud töötleja on täitnud kõik § 3 lõikes 4 sätestatud tingimused.

2. alljaotis
Avalike ülesannete täitmist oluliselt mõjutavad süsteemid

§ 11. Avalike ülesannete täitmist oluliselt mõjutavate süsteemide loetelu

Süsteemid, millel on oluline mõju riigi ja kohaliku omavalitsuse üksuse võimele täita avalikke ülesandeid, on:

1) e-toimiku süsteem;

2) elektrooniline kinnistusraamat;

3) äriregister;

4) riigi- ja kohaliku omavalitsuse asutuste riiklik register;

5) mittetulundusühingute ja sihtasutuste register;

6) kommertspandiregister;

7) Riigi Teataja infosüsteem;

8) elektrooniline kataster;

9) riigikassa infosüsteem;

10) maksukohustuslaste register;

11) rahvastikuregister;

12) sotsiaalkaitse infosüsteem.

§ 12. Avalike ülesannete täitmist oluliselt mõjutavate süsteemide pidamise nõuded

(1) Paragrahvis 11 nimetatud süsteemide andmekoosseis, vajadusel koos andmekoosseisu kasutamiseks vajaliku toimiva rakenduskihiga, varundatakse välisriigiga sõlmitud rahvusvahelise lepingu alusel regulaarselt välisriigis asuvasse turvalisse andmekeskusesse. Varundamise üksikasjad lepitakse kokku Eesti Vabariigi ja välisriigi vahelise andmete ja infosüsteemide majutamise kokkuleppega.

(2) Paragrahvis 11 nimetatud süsteemide kaitsetarve Eesti Infoturbestandardi tähenduses on väga suur (VS), kuid see ei välista varundamise lõike 1 kohaselt.

(3) Paragrahvis 11 nimetatud süsteemidele ei kohaldata § 3 lõiget 4 ning § 4 lõiget 3.

3. alljaotis
Rahvusvaheliseks sõjaliseks koostööks vajalikud süsteemid

§ 13. Rahvusvaheliseks sõjaliseks koostööks vajalike süsteemide loetelu ja nende pidamise nõuded

(1) Kaitseministeeriumi valitsemisalas rahvusvaheliseks sõjaliseks koostööks vajalike süsteemide loetelu ja nende turvameetmete kirjelduse kehtestab riigikaitse korraldamise eest vastutav minister määrusega.

(2) Küberturvalisuse seaduse § 7 lõike 5 ning käesoleva paragrahvi lõike 1 alusel kehtestatud määruses nimetatud süsteemidele ei kohaldata käesoleva määruse 2. peatükki, 3. peatüki 1. jagu ning 2. jao 1. ja 2. alljaotist.

4. peatükk
Rakendussätted

§ 14. Eesti Infoturbestandardi järgimise auditeerimise tähtajad

(1) Teenuse osutaja, kes on Vabariigi Valitsuse 20. detsembri 2007. a määruse nr 252 „Infosüsteemide turvameetmete süsteem“ § 9^1 lõike 1 alusel kohustatud läbi viima turvameetmete süsteemi rakendamise auditeerimist, on kohustatud esmakordse Eesti Infoturbestandardi järgimise auditeerimise läbi viima kahe aasta jooksul pärast viimast Vabariigi Valitsuse 20. detsembri 2007. a määruse nr 252 „Infosüsteemide turvameetmete süsteem“ § 9^1 lõike 1 alusel läbi viidud turvameetmete süsteemi auditeerimist.

(2) Teenuse osutaja, kes on Vabariigi Valitsuse 20. detsembri 2007. a määruse nr 252 „Infosüsteemide turvameetmete süsteem“ § 9^1 lõike 2 alusel kohustatud läbi viima turvameetmete süsteemi rakendamise auditeerimist, on kohustatud esmakordse Eesti Infoturbestandardi järgimise auditeerimise läbi viima kolme aasta jooksul pärast viimast Vabariigi Valitsuse 20. detsembri 2007. a määruse nr 252 „Infosüsteemide turvameetmete süsteem“ § 9^1 lõike 2 alusel läbi viidud turvameetmete süsteemi auditeerimist.

(3) Teenuse osutaja, kes on Vabariigi Valitsuse 20. detsembri 2007. a määruse nr 252 „Infosüsteemide turvameetmete süsteem“ § 9^1 lõike 3 alusel kohustatud läbi viima turvameetmete süsteemi rakendamise auditeerimist, on kohustatud esmakordse Eesti Infoturbestandardi järgimise auditeerimise läbi viima nelja aasta jooksul pärast viimast Vabariigi Valitsuse 20. detsembri 2007. a määruse nr 252 „Infosüsteemide turvameetmete süsteem“ § 9^1 lõike 3 alusel läbi viidud turvameetmete süsteemi auditeerimist, kuid mitte hiljem kui 1. jaanuar 2025.a.

(4) Käesoleva paragrahvi lõigetes 1-3 nimetamata teenuse osutaja on kohustatud esmakordse Eesti Infoturbestandardi järgimise auditeerimise läbi viima hiljemalt 1. jaanuar 2025. a.

§ 15. Määruse jõustumine

(1) Käesolev määrus jõustub 1. jaanuaril 2022. a.

(2) Käesoleva määruse §-id 6-10 jõustuvad 1. jaanuaril 2023. a.

VABARIIGI VALITSUS
MÄÄRUS

Vabariigi Valitsuse määruste muutmine seoses Eesti Infoturbestandardiga

Määrus kehtestatakse arhiiviseaduse § 13, avaliku teabe seaduse § 32^1 lõike 5, § 43^3 lõike 5, § 43^7 lõike 1 ning § 43^9 lõike 1 punkti 6, kodakondsuse seaduse § 9 lõike 6, keeleseaduse § 27 lõike 3, perioodi 2004–2006 struktuuritoetuse seaduse § 9 lõike 6, perioodi 2007–2013 struktuuritoetuse seaduse § 4 lõike 3, perioodi 2014–2020 struktuuritoetuse seaduse § 37 lõike 4, põhikooli- ja gümnaasiumiseaduse § 32 lõigete 1 ning 2, Vabariigi Valitsuse seaduse § 27 lõike 3 ja välissuhtlemisseaduse § 8 lõike 6 alusel.

§ 1. Vabariigi Valitsuse 22. detsembri 2011. a määruse nr 181 „Arhiivieeskiri“ muutmine

Määruse § 28 lõige 14 muudetakse ja sõnastatakse järgmiselt:

„(14) Digitaalarhivaalide säilitamisel tuleb juhinduda ettevõtlus- ja infotehnoloogiaministri xxx 2021. a määrusega nr yyy „Eesti Infoturbestandardi kehtestamine” sätestatud Eesti Infoturbestandardi rakendamisjuhendi tüüpmoodulite turvameetmetest vastavalt digitaalarhivaalide säilitamisel kasutatavatele infrastruktuuri, IT-süsteemide, võrkude ja rakenduste komponentidele ning infovarade kaitsetarbele.“.

§ 2. Vabariigi Valitsuse 3. oktoobri 2013. a määruse nr 145 „Eesti teabevärava eesti.ee haldamise, teabe kättesaadavaks tegemise, arendamise ning kasutamise nõuded ja kord“ muutmine

1) määruse § 13 lõike 1 punkti 14 täiendatakse pärast sõna „turbeaste“ sõnadega „või teenuse kaitsetarve Eesti Infoturbestandardi tähenduses;

2) määruse § 13 lõike 1 punkt 14 muudetakse ja sõnastatakse järgmiselt:

„14) teenuse kaitsetarve Eesti Infoturbestandardi tähenduses;“;

§ 3. Vabariigi Valitsuse 15. märtsi 2012. a määruse nr 26 „Infoturbe juhtimise süsteem“ muutmine

1) määruse § 1 lõige 2 muudetakse ja sõnastatakse järgmiselt:

„(2) Asutuse juht ja infoturbejuht juhinduvad oma tööülesannete täitmisel küberturvalisuse seadusest, käesolevast määrusest, Vabariigi Valitsuse xxx 2021. a määrusest nr yyy “Võrgu- ja infosüsteemide küberturvalisuse nõuded“ ning nimetatud määruse alusel vastu võetud ettevõtlus- ja infotehnoloogiaministri xxx 2021. a määruse nr yyy „Eesti Infoturbestandardi kehtestamine“ alusel kehtestatud Eesti Infoturbestandardist, Vabariigi Valitsuse 20. detsembri 2007. a määrusest nr 252 „Infosüsteemide turvameetmete süsteem”, rahvusvahelistest infoturbe halduse standarditest ja parimast praktikast.“;

2) määruse § 1 lõikes 2 jäetakse välja sõnad „Vabariigi Valitsuse 20. detsembri 2007. a määrusest nr 252 „Infosüsteemide turvameetmete süsteem”,“;

3) määruse § 4 lõike 4 punkti 3 täiendatakse pärast sõna „süsteemi“ sõnadega „või Eesti Infoturbestandardi“;

4) määruse § 4 lõike 4 punktis 3 jäetakse välja sõnad „infosüsteemide turvameetmete süsteemi“;

5) määruse § 4 lõike 4 punktis 6 jäetakse välja sõnad „nende nõuete järgi, mis on toodud Vabariigi Valitsuse 20. detsembri 2007. a määruse nr 252 „Infosüsteemide turvameetmete süsteem” alusel kinnitatud rakendamisjuhendis“.

§ 4. Vabariigi Valitsuse 28. veebruari 2008. a määruse nr 58 „Riigi infosüsteemi haldussüsteem“ muutmine

1) määruse § 18 lõike 2 punkti 18 täiendatakse pärast sõna „süsteemi“ sõnadega „või Eesti Infoturbestandardi“;

2) määruse § 18 lõike 2 punktis 18 jäetakse välja sõnad „infosüsteemide turvameetmete süsteemi või“.

§ 5. Vabariigi Valitsuse 31. juuli 2014. a määruse nr 121 „Struktuuritoetuse registri pidamise põhimäärus“ muutmine

Määruse § 12 lõige 2 esimest lauset muudetakse ja sõnastatakse järgmiselt:

„Registri turvaklass on K2T2S1.“.

§ 6. Vabariigi Valitsuse 14. veebruari 2013. a määruse nr 27 „Testide andmekogu asutamine ja põhimäärus“ muutmine

Määruse § 16 lõikes 4 jäetakse välja sõna „ISKE“.

§ 7. Määruse jõustumine

(1) Määrus jõustub 1. jaanuaril 2022. a.

(2) Määruse § 2 punkt 2, § 3 punktid 2, 4 ja 5 ning § 4 punkt 2 jõustuvad 1. jaanuaril 2023. a.

ETTEVÕTLUS- JA INFOTEHNOLOOGIAMINISTER
MÄÄRUS

Eesti Infoturbestandardi kehtestamine

Määrus kehtestatakse küberturvalisuse seaduse § 7 lõike 5 ning Vabariigi Valitsuse xxx määruse „Võrgu- ja infosüsteemide küberturvalisuse nõuded“ § 4 lõike 3 alusel.

§ 1. Eesti Infoturbestandardi kehtestamine

(1) Eesti Infoturbestandardi (E-ITS) dokumentatsioon on lisatud käesolevale määrusele.

(2) E-ITS-i dokumentatsiooni versioonis 1.00 on:

1) standardi dokumendid (sh alusohtude kataloog, auditeerimisjuhend, organisatsiooni infoturbe halduse süsteemi (ISMS) nõuded ja juhised, E-ITS-i rakendusjuhend, riskihaldusjuhend, üleminekujuhend infosüsteemide kolmeastmelise etalonturbe süsteemilt (ISKE) E-ITS-le ning muud juhendid);

2) etalonturbe kataloog;

3) seletav sõnaraamat.

§ 2. Määruse jõustumine

Määrus jõustub 1. jaanuaril 2022. a.

Lisa : Eesti Infoturbestandardi (E-ITS) versioon 1.00. [kättesaadav E-ITS portaalist: https://eits.ria.ee/]

ETTEVÕTLUS- JA INFOTEHNOLOOGIAMINISTER
MÄÄRUS

Eesti küberturvalisuse valdkonna tööstuse, tehnoloogia ja teadusuuringute koordineerimisüksuse määramine ja ülesannete täitmise kord

Määrus kehtestatakse küberturvalisuse seaduse § 5^1 lõike 3 alusel.

§ 1. Eesti küberturvalisuse valdkonna tööstuse, tehnoloogia ja teadusuuringute koordineerimisüksuse määramine

Eesti küberturvalisuse valdkonna tööstuse, tehnoloogia ja teadusuuringute koordineerimisüksus (edaspidi *TTT koordineerimisüksus*) küberturvalisuse seaduse § 5^1 lõike 2 tähenduses on Riigi Infosüsteemi Amet.

§ 2. Ülesannete täitmise kord

(1) Euroopa Parlamendi ja nõukogu määruse (EL) 2021/887, millega luuakse küberturvalisuse valdkonna tööstuse, tehnoloogia ja teadusuuringute Euroopa pädevuskeskus ning riiklike koordineerimiskeskuste võrgustik (ELT L 202, 08.06.2021, lk 1-31) artiklis 7 nimetatud ülesannete täitmisel järgib TTT koordineerimisüksus Majandus- ja Kommunikatsiooniministeeriumi riikliku küberturvalisuse osakonna (edaspidi *RKO*) esitatud suuniseid.

(2) Euroopa Parlamendi ja nõukogu määruse (EL) 2021/887 artikli 7 lõike 1 punkti b alusel küberturvalisuse valdkonna tööstuse, tehnoloogia ja teadusuuringute Euroopa pädevuskeskusele esitatava teabe kooskõlastab TTT koordineerimisüksus mõistliku aja jooksul RKO-ga.

(3) Euroopa Parlamendi ja nõukogu määruse (EL) 2021/887 artikli 7 lõike 3 alusel saadud toetust kasutab TTT koordineerimisüksus eelnevalt RKO poolt kinnitatud eelarve alusel. Eelarve kinnitamiseks esitab TTT koordineerimisüksus eelarve ettepaneku RKO-le.

(4) TTT koordineerimisüksuse ülesannete täitmise korda koordineerib ja koostööd RKO-ga korraldab RKO osakonnajuhataja.

§ 3. Määruse jõustumine

Määrus jõustub 1. jaanuaril 2022. a.

ETTEVÕTLUS- JA INFOTEHNOLOOGIAMINISTER
MÄÄRUS

Majandus- ja taristuministri määruste ning majandus- ja kommunikatsiooniministri määruse muutmine

Määrus kehtestatakse perioodi 2014–2020 struktuuritoetuse seaduse § 14 ja § 15 lõike 2 ning Vabariigi Valitsuse seaduse § 42 lõike 1 alusel.

§ 1. Majandus- ja taristuministri 15. aprilli 2015. a määruse nr 31 „Avalike teenuste pakkumise arendamiseks toetuse andmise tingimused ja kord“ muutmine

1) määruse § 4 täiendatakse punktiga 3^1 järgmises sõnastuses

„3^1) Eesti Infoturbestandard (edaspidi *E-ITS*) on infoturbe halduse süsteem vastavalt küberturvalisuse seaduse § 7 lõike 5 ning Vabariigi Valitsuse xxx 2021. a määruse „Võrgu- ja infosüsteemide küberturvalisuse nõuded“ § 4 lõike 3 alusel kehtestatud määrusele, arvestades viidatud Vabariigi Valitsuse määruse 2. peatükki;“;

2) määruse § 6 lõike 1 punkti 3 täiendatakse pärast sõna „süsteem““ sõnadega „või E-ITS-i“;

3) määruse § 7 lõike 2 punktides 1 ja 2 täiendatakse pärast sõna „ISKE“ sõnadega „või E-ITS-i“;

4) määruse § 12 lõike 1 punktis 10 täiendatakse pärast sõna „moodulid“ sõnadega „või E-ITS-i moodulid“;

5) määruse § 27 lõike 4 punktis 3 täiendatakse pärast sõnu „et ISKE“ sõnadega „või E-ITS-i“ ning pärast sõnu „alustatud ISKE“ sõnadega „või E-ITS-i“.

§ 2. Majandus- ja taristuministri 12. märtsi 2015. a määruse nr 21 „Nutika teenuste taristu arendamise toetamise tingimused ja investeeringute kava koostamise kord“ muutmine

1) määruse § 6 lõike 1 punktis 11 täiendatakse pärast sõna „süsteem““ sõnadega „või Eesti Infoturbestandardi“;

2) määruse § 7 lõike 2 punktis 1 täiendatakse pärast sõna „süsteemi“ sõnadega „või Eesti Infoturbestandardi“.

§ 3. Majandus- ja kommunikatsiooniministri 25. aprilli 2011. a määruse nr 28 „Riigi Infosüsteemi Ameti põhimäärus” muutmine

1) paragrahvi 8 lõiget 4 täiendatakse punktiga 3^1 järgmises sõnastuses:

„3^1) täidab küberturvalisuse seaduse § 5^1 lõike 2 tähenduses Eesti küberturvalisuse valdkonna tööstuse, tehnoloogia ja teadusuuringute koordineerimisüksuse ülesandeid sama paragrahvi lõike 3 alusel kehtestatud määruses sätestatud korras.“;

2) paragrahvi 13 lõike 1 punkti 7 muudetakse ja sõnastatakse järgmiselt:

„7) küberturvalisuse alase teadus- ja arendustegevuse korraldamine ja koordineerimine ning valdkonna teadus- ja uurimisasutustega koostöö tegemine teenistuse pädevuse piires.“.

§ 4. Määruse jõustumine

Määrus jõustub 1. jaanuaril 2022. a.

KAITSEMINISTER
MÄÄRUS

Rahvusvaheliseks sõjaliseks koostööks vajalike süsteemide loetelu ja nende turvanõuded

Määrus kehtestatakse küberturvalisuse seaduse § 7 lõike 5 ning Vabariigi Valitsuse xxx määruse „Võrgu- ja infosüsteemide küberturvalisuse nõuded“ § 13 lõike 1 alusel.

§ 1. Süsteemide loetelu

Kaitseministeeriumi valitsemisalas rahvusvaheliseks sõjaliseks koostööks vajalike süsteemide (edaspidi *süsteem*) loetelu on toodud määruse lisas „Rahvusvaheliseks sõjaliseks koostööks vajalike süsteemide loetelu“.

§ 2. Turvanõuded

(1) Süsteemi vastutav töötleja kehtestab süsteemi toimimiseks nõutavad turvanõuded.

(2) Turvanõuetega nähakse ette vähemalt:
1) süsteemide juurdepääsuõiguste haldamine, süsteemi kasutajate identifitseerimine ja autoriseerimine;
2) teenuse osutamiseks vajalikest andmetest regulaarsete varukoopiate tegemine ja protseduurid andmete varukoopiatest taastamiseks;
3) süsteeme käitava ja süsteemides käideldava tarkvara ajakohasus;
4) süsteemides läbiviidavate toimingute logid toimingu teostaja, toimingu liigi ja toimingu teostamise ajaga;
5) tarkvaralised ja riistvaralised lahendused süsteemide turvalisust ohustava tegevuse ja tarkvara tuvastamiseks ning tõrjumiseks;
6) protseduurid süsteemide turvalisuse või teenuse toimepidevuse taastamiseks.

(3) Turvanõuete täitmisel lähtutakse Kaitseministeeriumi valitsemisalas kehtestatud turvameetmetest ja Põhja-Atlandi Lepingu Organisatsiooni nõuetest või muudest rahvusvahelistest lepingutest tulenevatest nõuetest.

§ 3. Määruse jõustumine

Määrus jõustub 1. jaanuaril 2022. a.

Lisa Rahvusvaheliseks sõjaliseks koostööks vajalike süsteemide loetelu (asutusesiseseks kasutamiseks mõeldud teave)

RAHANDUSMINISTER
MÄÄRUS

Rahandusministri määruste muutmine seoses Eesti Infoturbestandardiga

Määrus kehtestatakse hasartmänguseaduse § 36 lõike 5 ja § 58 lõike 10 alusel.

§ 1. Rahandusministri 19. juuni 2012. a määruse nr 26 „Hasartmängukorraldaja elektroonilises arvestus- ja kontrollisüsteemis registreeritavate andmete loetelu ja sisestamise kord ning elektroonilise arvestus- ja kontrollisüsteemi Maksu- ja Tolliameti infosüsteemiga ühendamise kord“ muutmine

Määruse § 2 lõikes 2 jäetakse välja sõnad „infosüsteemide kolmeastmelise etalonturbe süsteemi (ISKE)“.

§ 2. Rahandusministri 7. aprilli 2004. a määruse nr 70 „Ühendusevälise riigi füüsilisele isikule võõrandatava kauba ekspordina käsitamise kord“ muutmine

1) määruse § 2 lõike 3^1 punkti 3 täiendatakse pärast sõna „tasemel“ sõnadega „või kaitsetarbele suur (S) Eesti Infoturbestandardi tähenduses ning sellest lähtuvatele turvameetmetele“;

2) määruse § 2 lõike 3^1 punktis 3 jäetakse välja sõnad „infosüsteemide kolmeastmeline etalonturbe süsteemi (ISKE) nõuetele vähemalt keskmisel (M) tasemel või“.

§ 3. Määruse jõustumine

(1) Määrus jõustub 1. jaanuaril 2022. a.

(2) Määruse § 2 punkt 2 jõustub 1. jaanuaril 2023. a.

TERVISE- JA TÖÖMINISTER
MÄÄRUS

Tervise- ja tööministri 6. märtsi 2019. a määruse nr 15 „Vee terviseohutuse infosüsteemi põhimäärus“ muutmine seoses Eesti Infoturbestandardiga

Määrus kehtestatakse rahvatervise seaduse § 14^6 lõike 4 alusel.

§ 1. Määruse muudatused

1) määruse § 5 lõiget 1 täiendatakse pärast sõna „nõuetele“ sõnadega „ning infosüsteemile määratud kaitsetarbele Eesti Infoturbestandardi tähenduses“;

2) määruse § 5 lõikes 1 asendatakse sõnad „riigi infosüsteemide turvameetmete süsteemi nõuetele ning infosüsteemile määratud kaitsetarbele Eesti Infoturbestandardi tähenduses“ sõnadega „Vabariigi Valitsuse xxx 2021. a määruse „Võrgu- ja infosüsteemide küberturvalisuse nõuded“ nõuetele“.

§ 2. Määruse jõustumine

(1) Määruse § 1 punkt 1 jõustub 1. jaanuaril 2022. a.

(2) Määruse § 1 punkt 2 jõustub 1. jaanuaril 2023. a.