

Esmased turvameetmed

- Käesolevas lisas sätestatakse määruse § 5¹ lõikes 1 loetletud turbevaldkondades rakendatavad esmased turvameetmed.
- Käesolevas lisas esitatud meetmed on ette nähtud kõigile küberturvalisuse seaduses loetletud teenuseosutajatele, kui määruses ei ole sätestatud teisiti.
- Teenuseosutaja võib käesolevas lisas sätestatud meetme asemel võtta kasutusele mõne muu samaväärse meetme riskide vähendamiseks.
- Teenuseosutaja ei pea käesolevas lisas sätestatud meetet rakendama, kui meede ei ole asjakohane või rakendatav ja kui ta on rakendamata jätmisega kaasnevad riskid teadvustanud.

1. Infoturbe korralduse valdkonnas peab teenuseosutaja:

- 1.1. määrama infoturbe eest vastutava isiku;
- 1.2. välja töötama võrgu- ja infosüsteemide turvareeglid, sealhulgas infoturbepõhimõtted, ning tutvustama neid personalile;
- 1.3. kontrollima regulaarselt, kas valitud turvameetmed vastavad tegelikule vajadusele ja kas turvameetmed on rakendatud. Turvameetmeid tuleb kontrolli tulemuste põhjal korrigeerida;
- 1.4. pidama infotehnoloogiavarade arvestust ja uuendama seda regulaarselt;
- 1.5. määrama kasutusel olevale infotehnoloogiaseadmele vastutava kasutaja.

2. Kasutajate teadlikkuse ja koolituse valdkonnas peab teenuseosutaja:

- 2.1. tutvustama personalile küberhügieeni- ja infoturbereegleid, hindama teadmisi ja tagama vastava koolituse, vajaduse korral perioodiliselt;
- 2.2. juhendama personali infotehnoloogiaseadmete kasutamisel;
- 2.3. kasutama võrgu- ja infosüsteemides personaalseid pääsuõigusi;
- 2.4. sulgema pääsuõigused või kontod, mille järele puudub vajadus või mida ei kasutata;
- 2.5. eelistama mitmeastmelist autentimist;
- 2.6. hoidma pääsuks vajalikke vahendeid, sealhulgas salasõnu ja räsisid, volitamata isikutele kättesaamatusena;
- 2.7. kasutama võrgu- ja infosüsteemis ainult selleks mõeldud ning heaks kiidetud seadmeid, teenuseid ja süsteeme;
- 2.8. kasutama infotehnoloogiaseadmeid ja andmekandjaid heaperemehelikult ning mitte jätma neid järelevalveta.

3. Andmete turbe valdkonnas peab teenuseosutaja:

- 3.1. hindama, millised andmed ning võrgu- ja infosüsteemid on vajalikud igapäevaseks kasutamiseks, ning kavandama asendusprotseduurid süsteemide tõrgete ja katkestuste korral;
- 3.2. välja töötama tööks vajalike andmete kasutamise reeglid, sealhulgas teiste isikutega andmete jagamise kohta;
- 3.3. tagama kasutatava teabe või teiste isikute edastatud teabe, sealhulgas ärisaladuse ja isikuandmete kaitse ning vajaduse korral kasutama ajakohast krüpteerimist;
- 3.4. eelistama digitaalset lahendust, mis kinnitab oluliste elektrooniliste andmete päritolu ja terviklust, sealhulgas digitaalne allkirjastamine;

- 3.5. rakendama andmetele juurdepääsu võimaldamisel teadmismajaduspõhist juurdepääsuhaldust;
- 3.6. varundama regulaarselt tööks vajalikke andmeid, hoidma varundatud andmeid töösüsteemist eraldi ja testima varukoopiast andmete taastamist;
- 3.7. tagama andmete kustutamise enne andmekandja kasutamise lõpetamist või edasiandmist.

4. Väliste partnerite halduse valdkonnas peab teenuseosutaja:

- 4.1. omama ülevaadet oma olulistest tarnijatest ja välistest teenuseosutajatest ning nende taustast. Saadud teabe põhjal tuleb rakendada asjakohaseid turvameetmeid, lähtudes riigi koostatud avalikest ohuhinnangutest ja riskianalüüsist;
- 4.2. kokku leppima tarnijatega, väliste teenuseosutajatega ja partneritega kirjalikult taasesitatavas vormis andmete vahetamiseks vajalikud turvanõuded ning kasutatava teenuse tingimused.

5. Küberintsidentide halduse valdkonnas peab teenuseosutaja:

- 5.1. koolitama personali, kuidas ära tunda intsidente, tuvastada nende mõju ja ulatust ning neid vältida ja intsidentide puhul toimida;
- 5.2. määrama isiku, kes koordineerib intsidentide lahendamist ning asjaomaste asutuste ja koostööpartnerite teavitamist ning on nende kontaktisik;
- 5.3. kokku leppima alternatiivsed teavituskanalid juhaks, kui tavapärane teabevahetus ei toimi.

6. Pilvteenuste ja veebirakenduste kaitse valdkonnas peab teenuseosutaja:

- 6.1. kasutama üksuses kinnitatud ja ajakohastatud veebibrausereid ning veebibrauseri laiendeid, millel on toimiv tootjapoolne tugi ja on rakendatud turvalised seadistused;
- 6.2. jagama pilvteenustes juurdepääsude jagamisel andmeid vaid identifitseeritud kasutajatele tööks vajalikus ulatuses;
- 6.3. järgima turvalise e-kirjavahetuse põhimõtteid, vältima tundmatute manuste või hüperlinkide avamist ja pöörama tähelepanu tundmatute saatjate usaldusväärsusele;
- 6.4. kasutama sõnumirakendustes, telefoni- ja videokõnede tegemisel üksuses kokku lepitud ja heaks kiidetud reegleid;
- 6.5. järgima brauseri turvahoiatusi ning kasutama vaid selliseid veebilehti ja rakendusliideseid, mille turvalisuses on enne veendunud;
- 6.6. pidama nimekirja kõigist kasutuses olevatest pilvteenustest koos teenuse pakkuja, kasutusotstarbe ja riskihinnangu kokkuvõttega.

7. Infotehnoloogiaseadmete kaitse valdkonnas peab teenuseosutaja:

- 7.1. kasutama ajakohast viirusetõrjet ja tulemüüri;
- 7.2. uuendama regulaarselt kasutatavaid operatsioonisüsteeme ja rakendusi;
- 7.3. pidama arvestust kasutatava tarkvara, selle turvahaavatavuste ja litsentside üle ning uuendama litsentse õigel ajal;
- 7.4. kasutama turvalist, usaldusväärset ja kehtiva toega tarkvara, sealhulgas eemaldama infotehnoloogiaseadmetest ja telefonidest tarkvara, mis on aegunud või mida ei kasutata;
- 7.5. eristama seadmetes kasutaja- ja süsteemi haldusõigusi ning kasutama tavapärases tegevuses vähem privilegeeritud kasutajatunnuseid;
- 7.6. tagama võrgu- ja infosüsteemide ning rakenduste turvasündmuste logimise ja logide kättesaadavuse;
- 7.7. krüpteerima olulist teavet töötleva seadme kõvaketta ja teavet sisaldavad välised kõvakettad ajakohast krüptograafilist meedet kasutades;
- 7.8. paigutama võimaluse korral seadmed nii, et need ei oleks kõrvalistele isikutele ligipääsetavad;

- 7.9. kasutama tööks vajalikes seadmetes, sealhulgas mobiilseadmes pääsukoodi või ekraanilukku;
- 7.10. kavandama meetmed juhuks, kui seade läheb kaotsi, varastatakse või läheb katki;
- 7.11. kustutama seadmest kogu teabe enne selle kasutusest kõrvaldamist ja utiliseerimist;
- 7.12. rakendama asjakohaseid lisaturvameetmeid oma serveri kaitsmiseks;
- 7.13. rakendama automaatikaseadme või muu andmesideühendusega seadme kasutamise korral lisaturvameetmeid või keelama seadmes andmeside kasutamise, sealhulgas kaughalduse;
- 7.14. hindama uute seadmete ning info- ja võrgusüsteemide soetamisel võimalikke riske ja rakendama juba plaanimise etapis asjakohaseid turvameetmeid.

8. Sideühenduste ja võrgu kaitse valdkonnas peab teenuseosutaja:

- 8.1. koostama arvutivõrgu skeemi, sealhulgas pidama võrguseadmete ning võrgule tuge pakkuvate isikute ja nende kontaktandmete arvestust;
- 8.2. piirama volitamata juurdepääsu infosüsteemidele ja seadmetele väliste võrkude kaudu, kasutades tulemüüri või samaväärset turvalahendust;
- 8.3. vältima volitamata isikule kaugjuurdepääsu andmist sisevõrgus või pilvteenustes töödeldavale teabele;
- 8.4. kasutama traadita kohtvõrgu ühenduste korral tugevat salasõna ja turvaprotokolli.

9. Füüsilise turbe valdkonnas peab teenuseosutaja:

- 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;
- 9.3. vältima ruumides kõrvaliste isikute liikumist saatjata, eelkõige ruumides, kus hoitakse seadmeid või töödeldakse andmeid;
- 9.4. pidama arvestust ruumidele, sõidukitele, hoonetele ja muule varale juurdepääsu võimaldavate vahendite üle, sealhulgas kaardid, koodid ja võtmed;
- 9.5. rakendama meetmeid hoonesse või ruumidesse loata sisenemise takistamiseks;
- 9.6. piirama juurdepääsu võrguseadmete, hooneautomaatika ja serveri asukohale, sealhulgas hoidma vastavaid tehnilisi ruume ja seadmeid lukustatuna.