Väljaandja:	Alutaguse Vallavalitsus
Akti liik:	määrus
Teksti liik:	algtekst-terviktekst
Redaktsiooni jõustumise kp:	14.12.2019
Redaktsiooni kehtivuse lõpp:	23.09.2023
Avaldamismärge:	RT IV, 11.12.2019, 1

Alutaguse Vallavalitsuse infoturbepoliitika

Vastu võetud 04.12.2019 nr 10

Määrus kehtestatakse kohaliku omavalitsuse korralduse seaduse § 30 lõike 1 punkti 3, avaliku teabe seaduse § 43 lõike 1, küberturvalisuse seaduse § 7 lõigete 1-3 ja §-de 8-9, isikuandmete kaitse seaduse § 14 punkti 6 alusel ning kooskõlas Vabariigi Valitsuse 20. detsembri 2007. a määrusega nr 252 „Infosüsteemide turvameetmete süsteem".

§ 1. Reguleerimisala

Määrusega kehtestatakse infoturbe poliitika üldised põhimõtted mida on kohustatud täitma Alutaguse Vallavalitsuse kui ametiasutuse ja vallavalitsuse hallatavate asutuste (edaspidi koos *asutus*) teenistujad, töötajad, töövõtu- või muu lepingu alusel teenust osutavad isikud ning kõik teised isikud, kes osalevad asutuse töös.

§ 2. Eesmärgid

(1) Infoturbe poliitika eesmärk on kehtestada üldised suunised infovarade kaitsmiseks rünnete ja ohtude eest. Infoturbe poliitika alusel koostatakse infoturvet reguleerivad eeskirjad, juhendmaterjalid, korrad ja muud dokumendid.

(2) Infoturbe põhieesmärgid on:
1) kaitsta infovarasid ohtude eest;
2) tagada andmete väärtuste ja omaduste säilimine;
3) tagada asutuse infosüsteemide käideldavus;
4) minimeerida riske;
5) tagada õigusaktidele vastavus.

(3) Andmete tähendus ja väärtus määratakse infosüsteemide kolmeastmelise etalonturbe (edaspidi *ISKE*) metoodika alusel.

§ 3. Mõisted

Infoturbe kirjeldamisel kasutatakse mõisteid järgmises tähenduses:
1) infovara – informatsioon, andmed ja nende töötlemiseks vajalikud infotehnoloogilised rakendused ning tehnilised vahendid;
2) turvameetmed – organisatsioonilised toimingud ja vahendid, tehnilised protsessid ja tehniliste vahendite rakendamine andmete ja infosüsteemide turvalisuse saavutamiseks ja säilitamiseks;
3) infoturve – turvameetmete loomise, valimise ja rakendamise protsesside kogum;
4) infosüsteem – andmeid töötlev, salvestav või edastav tehniline süsteem koos tema normaalseks talitluseks vajalike vahendite, ressursside ja protsessidega;
5) andmekogu – infosüsteemis töödeldavate korrastatud andmete kogum;
6) ISKE − infoturbe metoodika, mida rakendatakse andmekogude pidamisel kasutatavatele infosüsteemidele ning nendega seotud infovaradele turvalisuse tagamiseks;
7) krüpteerimine – andmete muundamine matemaatilise algoritmi abil;
8) varundamine – meetmete komplekt võimaldamaks programme või andmeid taastada teadaoleva hetkeseisuni;
9) turvaintsident – sündmus või sündmused, millega kaasneb andmete või muude infovarade käideldavuse, tervikluse või konfidentsiaalsuse kadu või tekib oluline oht andmete käideldavuse, tervikluse või konfidentsiaalsuse kao tekkeks;
10) väline andmekandja – igasugune optiline, elektromagnetiline, pooljuhipõhine tehniline seade mis võimaldab andmeid salvestada ja transportida arvutite jt infotehnoloogiliste seadmete vahel ning mis ühendub juhtmega või juhtmevabalt arvuti või IT-seadme külge (näiteks CD, DVD, mälukaart, usb pulk, väline kõvaketas, nutitelefon jne).

§ 4. Infoturbe rakendamine

(1) Infoturbe rakendamise eest vastutab asutuse juht kehtestades infoturvet reguleerivad juhised ning rakendades infoturbe juhtimise süsteemi oma asutuses.

(2) Igal infovaral on vastutaja, kes määrab infovara turbevajaduse ja korraldab infoturbe nõuete täitmist.

(3) Iga infovara kasutaja vastutab infoturbe meetmete rakendamise eest, täidab infoturbe nõudeid ja rakendab asjakohaseid turvameetmeid.

(4) Avastatud turvaintsidentidest teavitatakse kokku lepitud teavitusskeemide kaudu.

(5) Tahtliku infoturbenõuete eiramise, infovarade mittesihipärase kasutamise või avastatud turvaintsidendist teatamata jätmise eest vastutab nõudeid rikkunud isik.

§ 5. Turvariskid

Turvariskide hindamisel rakendatakse ISKE metoodikat. Ohuallikateks infosüsteemidele võivad olla:
1) puudused infrastruktuuris – ebapiisav kaitse füüsiliste ohtude eest (näiteks kuum, külm, elektrikatkestus, vesi) või turbe füüsiliste meetmete osaline rakendamine;
2) puudused infotehnoloogias – süsteemide või seadmete tõrked (näiteks serveririke või võrguühenduse katkestus); seadmete paigutus; süsteemide jõudlus; ülepingutatud turvameetmed;
3) puudused töös − vead, mida töötajad teevad turvanõuete järgimisel (näiteks antakse edasi ligipääsuõigusi või taotletakse tarbetuid ligipääsuõigusi, ei järgita töö- ja eraasjade lahususe põhimõtet);
4) puudused töökorralduses – juhtumid, kus järgitakse turvanõuete täitmise reegleid puudulikult või ei täideta neid; kasutusjuhendid või süsteemikirjeldused on ebaselged või puuduvad; süsteemile juurdepääsu reguleerimise vahend ehk parool on nõrk või ebapiisav; arvutisse on paigaldatud volitamata tarkvara;
5) turvaründed;
6) vääramatu jõud.

§ 6. Turvariskide vähendamine

(1) Riskide vähendamiseks võetakse kasutusele järgmised meetmed:
1) füüsilised meetmed ruumidele (näiteks uste, akende ja lukkudega seotud abinõud);
2) organisatsioonilised meetmed töötajatele (näiteks protseduurireeglid, korrad ja eeskirjad turvanõuete täitmiseks);
3) infotehnoloogilised meetmed infosüsteemidele ja andmekogudele (näiteks ligipääsuõiguste andmise ja kasutamisega, viirusetõrjega, krüpteerimisega, varukoopiate tegemise ja ID-kaardi kasutamisega seotud abinõud).

(2) Andmete töötlemiseks asutuses kasutatakse vaid asutuse poolt lubatud riistvara- ja tarkvarastandardile vastavaid infotehnoloogilisi vahendeid. Asutuse sisevõrku ei tohi ühendada asutusele mittekuuluvaid seadmeid.

§ 7. Infoturbe meetmete rakendamine

(1) Asutuse infovarade riskihaldus põhineb ISKE-l. Selle alusel määratakse turvameetmed, mida tuleb rakendada infovaradele ettenähtud turvataseme saavutamiseks ja säilitamiseks.

(2) Kui mõnda turvameedet ei ole võimalik või otstarbekas rakendada, peab leidma alternatiivse meetme riski vähendamiseks.

(3) Kui infovara omanik või valdaja leiab, et ISKE-põhisest riskianalüüsist ei piisa, koostatakse lisaks detailne riskianalüüs, kus vaadatakse eraldi iga infovarale mõjuvat ohtu, hinnatakse ohu realiseerumise tõenäosust, selgitatakse välja suuremad riskid ja võetakse vajaduse korral kasutusele spetsiifilised meetmed nende vähendamiseks.

§ 8. Turvaintsidendid

(1) Turvaintsidendist või selle ohust peab töötaja koheselt teavitama asutuse andmekaitsespetsialisti, IT tuge ja enda vahetut juhti, töövälisel ajal enda vahetut juhti.

(2) Kui turvaintsidendi lahendamise käigus avastatakse kuriteo, väärteo, distsiplinaarsüüteo või töölepingu rikkumise tunnuseid, antakse juhtum edasi menetlemiseks asjaomase õigusega järelevalveasutusele või isikule.

(3) Turvaintsidentide haldus sätestatakse vallavalitsuse korraldusega.

§ 9. Pääsuõigused

(1) Ligipääs infovaradele tagatakse vaid volitatud kasutajatele.

(2) Pääsuõiguste jagamisel lähtutakse ametialase, tööalase või õppealase vajaduse põhimõttest.

(3) Pääsuõiguste taotlemisel ja seadistamisel lähtutakse võimalusel kohustuste lahususe printsiibist, kus pääsuõiguste taotleja ei saa olla pääsuõiguste seadistaja. Taotletud ning seadistatud ja töötajale antud pääsuõigused kinnitatakse asutuse juhi käskkirjaga.

(4) Pääsuõiguste jagajad võtavad kasutusele protseduurid, reeglid või muud mehhanismid, mis tagavad pääsuõiguste tühistamise, kui infosüsteemi kasutaja tööülesanded muutuvad, ta kaotab usalduse või tema töösuhe lõppeb.

(5) Reeglid, mille järgi valitakse salasõna, selle kehtivus ja muud parameetrid, kehtestatakse kas infosüsteemi kasutamise korra või mõne teise kohase juhendmaterjaliga.

§ 10. Krüpteerimine

(1) Asutusesiseseks kasutamiseks mõeldud info edastamisel läbi välisvõrkude peab see olema krüpteeritud.

(2) Krüpteerimise detailid sätestatakse infosüsteemide kasutamise korras.

§ 11. Viiruse- ja pahavaratõrje

(1) Kõikidele infosüsteemidele rakendatakse viiruse- ja pahavaratõrjet.

(2) Viiruse- ja pahavaratõrje andmebaase uuendatakse regulaarselt.

(3) Viirustõrjesüsteem peab olema keskhallatav.

§ 12. Infosüsteemide kasutusele võtmine ja muudatused

(1) Infosüsteemid ja nende muudatused testitakse enne kasutusele võtmist.

(2) Infosüsteemidele rakendatakse vajalikke turvameetmeid.

§ 13. Varundamine

(1) Andmete varundamise ja taastamise nõuded kehtestatakse vallavalitsuse korraldusega.

(2) Andmekogude varundusnõuded võib kehtestada igale andmekogule eraldi ja need kinnitab asutuse juht.

(3) Hävitatavad andmed kustutatakse turvaliselt sellisel viisil, mis välistab nende taastamise.

§ 14. Ruumide turve

(1) Ligipääs ruumidele tagatakse töövajaduse ja vastutuse alusel vastavalt asutuse töökorralduse reeglitele.

(2) Infoturbe seisukohalt olulised ruumid peavad olema valvestatud.

(3) Töövälisel ajal valvatakse hooneid ja ruume nii füüsiliselt kui ka elektrooniliselt. Vajadusel rakendatakse turvameetmeid ka territooriumi kaitseks.

§ 15. Kaugtöö

(1) Kaugtööl tuleb järgida asutuses kehtivat infosüsteemi kasutamise korda ning töökorralduse reegleid. Töökoha ressurssidega võib ühendust pidada ainult turvatud andmeside kaudu.

(2) Kaugtööl kasutatav tööalane teave tuleb hoida kättesaamatuna kolmandatele isikutele, sealhulgas pereliikmetele.

(3) Kaugtööl kasutatavad arvutid ja seadmed peavad vastama asutuse infoturbe nõuetele.

§ 16. Rakendussätted

(1) Infoturbe poliitika rakendamiseks vajalikud rakendusaktid kinnitab vallavalitsus või asutuse juht. Rakendusaktid peavad tuginema infoturbepoliitikale ja olema kooskõlas õigusaktidega.

(2) Alutaguse Vallavalitsuse 21.02.2019. a määrus nr 4 „Alutaguse Vallavalitsuse infoturbepoliitika“ tunnistatakse kehtetuks.

(3) Määrus jõustub kolmandal päeval pärast Riigi Teatajas avaldamist.

Tauno Võhmar
Vallavanem

Lehti Targijainen
Vallasekretär