Väljaandja:	Mustvee Vallavalitsus
Akti liik:	määrus
Teksti liik:	algtekst-terviktekst
Redaktsiooni jõustumise kp:	12.08.2019
Redaktsiooni kehtivuse lõpp:	Hetkel kehtiv
Avaldamismärge:	RT IV, 09.08.2019, 1

Mustvee Vallavalitsuse infoturbepoliitika

Vastu võetud 31.07.2019 nr 12

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

§ 1. Eesmärk ja sisu

(1) Infoturbepoliitika eesmärk on luua raamistik infoturbe korraldamiseks, et tagada Mustvee Vallavalitsuse (edaspidi *asutus*) infovarade käideldavus, terviklus ja konfidentsiaalsus kokkulepitud tasemel.

(2) Infoturbepoliitika sõnastab infoturbe põhimõtted, nende saavutamise suunised, infoturbe korralduse loogika ning peamiste infoturbemehhanismide rakendamise asutustes.

(3) Infoturbepoliitika järgib infotehnoloogia häid tavasid, parimaid praktikaid ja infosüsteemide kolmeastmelise etalonturbe süsteemi (edaspidi ISKE) suuniseid, mudeleid ja mõisteid. Infoturbepoliitikas on kasutatud standardseid infoturbetermineid selles tähenduses, nagu neid kasutatakse ISKE kehtivas versioonis.

§ 2. Kasutusulatus ja vastutus

(1) Infoturbepoliitika väljatöötamise ja vajaduspõhise uuendamise eest vastutab Mustvee Vallavalitsuse IT-spetsialist.

(2) Poliitika laieneb kõigile asutuste teenistujatele (nii ametnikele kui töötajatele) ja kehtib kõikides asutuste füüsilistes asukohtades, samuti tuleb antud põhimõtteid arvestada koostöös väliste teenusepakkujatega.

(3) Iga asutuse teenistujatele kohalduvad täpsemad infoturbe reeglid sätestatakse asutuse infosüsteemi kasutamise korraga (edaspidi ISKK), mis lähtuvad käesolevas infoturbepoliitikas toodud peamistest reeglitest.

§ 3. Viited

(1) Kehtiv ISKE versioon https://iske.ria.ee/.

(2) Krüptograafiliste algoritmide kasutusvaldkondade ning elutsükli viimane uuring https://www.ria.ee/ee/kruptograafiliste-algoritmide-elutsukli-uuringud.html.

§ 4. Mõisted

(1) **Andmekandja**– vahend informatsiooni salvestamiseks, säilitamiseks ja taaskasutamiseks.

(2) **Andmete varundamine**(*backup*) – andmetest varukoopiate tegemine, et võimaldada andmete taastamist arvutites ja -süsteemides.

(3) **Avariitaasteplaan**(*Disaster Recovery Plan*) – üksikasjalik käitumisjuhend asutuse infosüsteemi võimaliku avarii puhuks, mille eesmärgiks on minimeerida avariist tingitud kahjusid. Avariitaasteplaan koostatakse nii, et avarii korral infosüsteemi kriitilise tähtsusega osade töövõime säiliks või taastuks võimalikult lühikese ajaga.

(4) **Infoturbeintsident**– realiseerunud oht, mis põhjustab asutusele/asutuse infovarale kahju, mis võib olla: rahaline, konfidentsiaalsete andmete lekkimine, andmete hävimine, tööseisak, asutuse maine kahjustamine.

(5) **Infovara**– informatsioon, andmed ja nende töötlemiseks vajalikud infotehnoloogilised rakendused ning tehnilised vahendid.

(6) **Infosüsteem**– inimestest, tark- ja riistvarast koosnev süsteem, mis töötleb ja tõlgendab infot.

(7) **Infoturbejuht**– teenuseosutaja infoturbejuht või asutuse infoturbe eest vastutav isik.

(8) **Kasutaja**– kõik isikud, kellel on lähtuvalt oma teenistus-, töö- või praktikaülesannetest õigus IT teenuste (sh rakenduste) kasutamiseks.

(9) **Krüpteerimine**– informatsiooni kaitsmise võimalus, muutes andmed loetamatuks ja kasutamiskõlbmatuks inimesele, kellel puudub vastav dekrüpteerimisvõti.

(10) **Teenuslepe**– asutuse ja teenuseosutaja vaheline infotehnoloogia- ja kommunikatsiooniteenuste (edaspidi IT) tingimuste ning tasemete koostöö kokkulepe.

(11) **Teenuse omanik**- isik, kes vastutab oma (töö) protsessi nõuetekohase toimimise, sh rakenduse, funktsionaalse toimimise ning rakenduses sisalduvate andmete töötlemise õigsuse ning lõppkasutajate koolituse eest. Omanikku esindab tavaliselt struktuuriüksuse juht.

(12) **Teenuseosutaja**– asutusesisene või väline infotehnoloogia- ning kommunikatsiooniteenuste pakkuja.

(13) **Tulemüür**– tarkvara või seade, mis turvakaalutlustel piirab ja reguleerib võrguliiklust arvutivõrgus või võrkude vahel vastavalt seadistatud reeglitele. Tulemüüri esmane otstarve on väljastpoolt juurdepääsu takistamine ressurssidele, millele pole sellist juurdepääsu ette nähtud.

(14) **Turvaaudit**– infoturbe vastavuse kontroll, mida kasutatakse IT-süsteemi infoturbe asjakohase toimetaseme tagamiseks kogu IT-projekti või -süsteemi eluea kestel.

(15) **Virtuaalne privaatvõrk**ehk VPN (Virtual Private Network) on privaatne ja turvaline arvutivõrk, mille loomiseks kasutatakse avalikku telekommunikatsiooni infrastruktuuri.

§ 5. Infoturbe põhimõtted

(1) Infoturbe tagamise eest asutuses vastutab asutuse juht.

(2) Kõik infoturvet puudutavad muudatused tuleb kooskõlastada infoturbejuhiga.

(3) Asutuste infovarade kaitse tuleb tagada vastavalt nende väärtusele ja Eesti Vabariigis kehtivatele õigusaktidele.

(4) Infoturbe korraldamise eelduseks on, et mitte ükski turvameede ei loo kunagi absoluutset turvalisust, need vaid vähendavad turvariski, st tõenäosust, et andmete terviklus, käideldavus või konfidentsiaalsus saavad kahjustatud. Infosüsteemi turvalisus loetakse piisavaks, kui jääkrisk on asutuse jaoks aktsepteeritaval tasemel (võrreldes varade väärtusega ja turvameetmete maksumusega). Kui infosüsteemi funktsionaalsus on asutuse tegevuses kriitilise tähtsusega, infosüsteemi asendus- ja arenduskulud on ebamõistlikult suured või kui infovarasid ähvardab kõrge risk, viiakse vajadusel läbi detailne riskianalüüs.

(5) Iga asutus on kohustatud tagama kõikide enda käsutuses olevate infovarade kaitse vastavalt ohtude realiseerumise tõenäosusele ja kaitstavate varade väärtusele.

(6) Asutuse teenistujate teadlikkuse tõstmine ja motiveerimine on infoturbe peamine tagatis. Asutus viib läbi asutuste teenistujatele kohustuslikke regulaarseid infoturbealaseid koolitusi.

(7) Infoturbe nõuetega tuleb arvestada infosüsteemide kõikides arendamise etappides, samuti nende soetamisel.

(8) IT-spetsialist planeerib ja teostab turvaauditeid ning põhjendatud vajadusel viib läbi erakorralisi kontrolle.

(9) Infoturbeintsidendi või intsidendiohu ilmnemise korral peab teenistuja sellest viivitamatult teatama IT-spetsialistile.

(10) Kõik infoturbeintsidendid fikseeritakse ja olulisematest teavitab IT-spetsialist valitsemisala asutusi ning Riigi Infosüsteemi Ametit (edaspidi *RIA*).

(11) Kõigi infoturbeintsidentide osas korraldab IT-spetsialist menetluse, mille eesmärgiks on tuvastada intsidendi põhjused, tagajärjed ja leida lahendused tulevikus sarnaste intsidentide vältimiseks.

§ 6. Arvutitöökoht ja selle kasutamine

(1) Asutuse seadmetes kasutatav tarkvara peab olema hangitud legaalselt. Kõik infovarade kasutusviisid peavad olema legaalsed.

(2) Kõikidele asutuse arvutitöökoha seadmetele on paigaldatud tulemüüritarkvara ning keskselt hallatav viirusetõrje tarkvara, mille eemaldamine või välja lülitamine on keelatud.

(3) Asutuses osutatavaid internetist kättesaadavaid teenuseid (nt veebipõhine meiliteenus OWA) on lubatud kasutada ka isiklikest seadmetest. Isikliku seadme kasutamisel vastutab kasutaja ise infoturbe meetmete asjatundliku ja õigeaegse rakendamise eest.

(4) Kui asutuse andmeid sisaldavad seadmed antakse üle hoolduseks või remondiks välisele teenusepakkujale, tagab teenuseosutaja andmete turvalisuse, eemaldades seadme andmekandja ja hoiustades selle, kui see on tehniliselt võimalik. Kui seade antakse üle tervikuna välisele teenusepakkujale, tuleb seadme andmekandjatel sisalduv informatsioon turvaliselt kustutada, kui see on tehniliselt võimalik.

§ 7. Andmete kaitsmine

(1) Ametialaselt kasutatavad andmekandjad (nt väline kõvaketas, USB pulk, DVD jms) peavad olema selgelt ja arusaadavalt märgistatud.

(2) Käibelt kõrvaldatud või taaskasutatavatel andmekandjatel olevad andmed kustutab teenuseosutaja viisil, mis väldib juurdepääsupiiranguga andmete hilisema taastamise. Sellise kustutamisviisi puudumisel korraldab teenuseosutaja käibelt kõrvaldatud andmekandja füüsilise hävitamise ning hävitamise protokollimise kirjalikult.

(3) Kõik tarbetud paberkandjal olevad tööalased dokumendid tuleb hävitada paberihundis või muul selleks ette nähtud turvalisel viisil.

(4) Kasutajatel on lubatud kasutada ainult Eesti riigi poolt hallatavaid pilveteenuseid ja asutuse poolt sõlmitud lepingu alusel kasutatavaid pilveteenuseid kooskõlas ISKK-ga. Muudes pilveteenustes tööalase informatsiooni hoidmine on keelatud.

(5) Informatsiooni kaitsmiseks tuleb andmed krüpteerida, kui seda nõuab andmete iseloom lähtudes seejuures parimatele infotehnoloogiaalastele praktikatele ja tuginedes RIA soovitustele ning viimasele „Krüptograafiliste algoritmide kasutusvaldkondade ning elutsükli uuringule“.

(6) Teenuseosutaja krüpteerib kõikide sülearvutite, samuti väljaspool asutuse arvutivõrku asuvate lauaarvutite kõvakettad ja konfidentsiaalseid andmeid sisaldavate mobiiltelefonide ning tahvelarvutite püsimälu.

(7) Teenuseosutaja varundab asutuse infosüsteemides sisalduvaid andmeid. Andmete varundussüsteem võimaldab säilitada andmete täielikku või osalist koopiat teenuskaardil kokku lepitud tingimustel ning aja jooksul.

(8) Kriitiliste infovarade jaoks koostatakse taasteplaan, mille koostamise eest vastutab teenuseosutaja vastava süsteemi administraator. Taasteplaani aluseks olevate ärireeglite koostamise eest asutuse vastutab teenuse omanik.

(9) Kõik infosüsteemi olulised osad, sh võrguseadmed ja püsikaabeldus, peavad olema arusaadavalt tähistatud ja dokumenteeritud. Kõik ISKKist või käesoleva poliitika põhimõtetest tulenevad erandid tuleb samuti dokumenteerida.

§ 8. Ressurssidele juurdepääs

(1) Informatsioon, millele on määratud juurdepääsupiirang, peab olema kättesaadav ainult selleks volitust omavatele isikutele selles ettenähtud korras ja ulatuses.

(2) Igale teenistujale on loodud parooliga kaitstud individuaalne kasutajakonto, mis koos ID-kaardi ja mobiil-IDga moodustavad kasutaja identiteedi asutuse sisevõrgus. Teenuseosutaja loodud kasutajakontot kasutatakse juurdepääsu andmiseks kõikjal, kus tehniliselt võimalik. Iga teenistuja vastutab oma identiteedi kaitse eest. Sama kasutajakonto kasutamine mitme isiku poolt ei ole lubatud.

(3) Juurdepääs ressurssidele on rollipõhine, põhjendatud vastavalt tööalasele vajadusele. Ülemääraste õiguste taotlemine ja andmine ei ole lubatud.

(4) Teenusekontosid tohib kasutada vaid teenuste autentimiseks.

(5) Algparoolide kasutamine infosüsteemides on keelatud ja need tuleb vahetada esimesel sisselogimisel.

(6) Teenistujal on keelatud digitaalselt säilitada või edastada tööga seotud paroole vabatekstina (nt e-postiga krüpteerimata kujul). Samuti pole krüpteerimata kujul lubatud konfidentsiaalseid dokumente saata vabatekstina ega transportida asutuse ruumidest välja välistel andmekandjatel.

(7) Teenuseosutaja loob kõikidele infosüsteemidele avariikasutajakontod ja -paroolid, mis salvestatakse keskses paroolihaldussüsteemis. Keskse paroolihaldussüsteemi puudumisel tuleb avariikasutajakontosid ja -paroole säilitada kaitsekapis suletud ümbrikus.

(8) Kõikjal, kus võimalik, on paroolide regulaarne vahetamine tehniliselt jõustatud.

(9) Paroolid tuleb vahetada maksimaalselt iga 90 päeva tagant. Nõue ei kehti teenusekontodele ning avariiparoolidele, mida tuleb muuta viivitamatult juhul, kui nad saavad teatavaks isikutele, kellel puudub selleks põhjendatud tööalane teadmisvajadus või regulaarselt üks kord aastas.

(10) Autentimiseks kasutatavaid krüptograafilisi võtmeid tuleb vahetada minimaalselt regulaarselt üks kord aastas.

(11) Reeglina pole tavakasutajal oma kasutuses olevates töövahendites administraatori õiguseid.

(12) Süsteemiadministraatoritel on eraldi kasutajakonto administratiivsete toimingute tegemiseks, mida ei tohi kasutada kaugjuurdepääsu saavutamiseks.

(13) Kaugjuurdepääs ehk kaugtöö on asutuses lubatud üle virtuaalse privaatvõrgu (ehk VPNi) teenuseosutaja poolt väljastatud seadmetest.

(14) VPNi kaudu kasutatavate teenuste nimekirja kinnitab asutuse infoturbejuht, selle puudumisel juhtkond.

(15) Serveri- ja kommunikatsiooniruumid peavad vastama tingimustele, mis tulenevad seal töödeldavate andmete kõrgemast ISKE klassist. Serveri- ja tehnikaruume ei tohi märgistada üldarusaadavalt.

(16) Välise teenusepakkuja personali tohib lubada serveri- ja tehnikaruumidesse ainult koos saatjaga, kellel on volitatud ligipääs. Nimetatud isikute järelevalveta serveri- või tehnikaruumi jätmine on keelatud.

(17) Juurdepääsude haldus peab olema regulaarselt kontrollitud, tuvastatav ja jälgitav.

(18) Teenuseosutaja logib ressursside poole pöördumisi või pöörduskatseid, mis sisaldavad minimaalselt infot nende aja, lähtekoha, tegija ja tegevuse kohta. Logide säilitamine on kooskõlastatud asjasse puutuvate teenuse omanikega. Logidel on ajatembeldamise ning krüptoaheldamisega tagatud tõestusväärtus (ehk nn logiandmete muutmise lukustamise võimalus) kõikjal, kus see on tehniliselt võimalik ja andmete iseloomust tulenevalt põhjendatud.

§ 9. Arvutivõrgu turvalisuse tagamine

(1) Asutuse sisevõrk on välisvõrgust eraldatud tulemüüriga. Asutuse sisevõrk on minimaalselt jaotatud tulemüüriga eraldatud tsoonideks: sisevõrk serveritele; iga asutuse tööjaamadele; traadita võrgule; asutuse VPNi klientidele; välise teenusepakkujate VPNi ühendustele; serveritele, mis on kättesaadavad välisvõrgust.

(2) Asutuse sisevõrgus asuvad seadmed ei tohi olla otse kättesaadavad väljastpoolt, välja arvatud seadmed, mis asuvad just selleks otstarbeks loodud võrgutsoonides (demilitarized zone, DMZ).

(3) Arvutivõrku ühendatud seade ei tohi olla samaaegselt mitmes võrgutsoonis (nt sülearvuti ei tohi samaaegselt kasutada traadita ja traadiga internetti). Nõue ei kehti seadmetele (nt tulemüür, võrgujaotur või virtualiseerimishost), kus erinevates võrgutsoonides olemine on nende normaalse toimimise osa.

(4) Asutuse sisevõrku võõrarvutite ühendamine pole lubatud.

§ 10. Infoturbe põhimõtete muutmine

(1) Infoturbe põhimõtted vaadatakse üle vajaduse korral, kuid vähemalt kord kahe aasta jooksul.

(2) Infoturbepoliitikat muudetakse kui:
1) seda nõuavad auditi tulemused;
2) muudatuse vajadus tuleneb ISKE uue versiooni ilmumisest;
3) muudatuste vajaduse tingivad olulised tehnilised, organisatsioonilised või õiguslikud muutused või muud sisemised või välised asjaolud.

§ 11. Rakendussätted

Määrus jõustub kolmandal päeval pärast Riigi Teatajas avaldamist.

Märt Kraft
vallavanem

Marju Soop
jurist vallasekretäri ülesannetes