Väljaandja:	Võru Linnavalitsus
Akti liik:	määrus
Teksti liik:	terviktekst
Redaktsiooni jõustumise kp:	25.12.2012
Redaktsiooni kehtivuse lõpp:	Hetkel kehtiv
Avaldamismärge:	RT IV, 12.12.2012, 19

Võru Linnavalitsuse infoturbepoliitika

Vastu võetud 30.06.2010 nr 12
jõustumine 01.08.2010

Muudetud järgmiste aktidega

Vastuvõtmine	Avaldamine	Jõustumine
05.12.2012		25.12.2012

Määrus kehtestatakse "Kohaliku omavalitsuse korralduse seadus" § 30 lg 1 p 3 ja Vabariigi Valitsuse 20. detsembri 2007. a määrus nr 252 "Infosüsteemide turvameetmete süsteem" § 2 alusel.
[- jõust. 25.12.2012]

§ 1. EESMÄRK JA PÕHIMÕTTED

(1) Infoturbepoliitika määratleb ametiasutuse Võru Linnavalitsus (edaspidi *linnavalitsus*) suunised oma infovarade turvalisuse tagamisel. Linnavalitsus püüab piisavate turvameetmete rakendamisega kõige tõenäolisemate ohtude tingimustes vältida oma infovarade ja oma maine kahjustamist ning tagada katkestusteta tegevus oma ülesannete saavutamiseks. Valitud turvameetmed peavad aitama täita õigusaktidest tulenevaid turvanõudeid ning olema majanduslikult õigustatud ning nende häiriv toime linnavalitsuse tegevusele ja ta töötajate tööle peab olema võimalikult väike.

(2) Infoturbepoliitika sõnastab turbe eesmärgid, nende saavutamise suunised, üldise turbekorralduse ja -strateegia ning peamiste turvamehhanismide rakendamise poliitika.

(3) Linnavalitsus lähtub oma infoturbe korraldamisel info- ja kommunikatsioonitehnoloogia (edaspidi *IT*) halduse headest tavadest ja infosüsteemide kolmeastmelisest etalonturbe süsteemi (edaspidi *ISKE*) juhistest. Turvadokumentide koostamisel kasutatakse ISKE mudeleid ja mõisteid.

(4) Linnavalitsuse infoturbepoliitika hõlmab kõiki Linnavalitsuse struktuuriüksusi ja kehtib kõigis Linnavalitsuse struktuuriüksuste füüsilistes asukohtades.

§ 2. MÕISTED

(1) Infoturve – teabe ja infosüsteemide kaitsmine loata juurdepääsu, kasutamise, avaldamise, muutmise või hävitamise eest.

(2) Infovara – informatsioon, andmed ja nende töötlemiseks vajalikud rakendused. Andmebaas on korrastatud infokogum, kusjuures pole oluline, mis tüüpi see info on.

(3) Etalonturve – turvameetmestik, mille rakendamine on vajalik andmete turvalisuse saavutamiseks ja säilitamiseks.

(4) Logi – arvuti tegevuse päevik, mida kasutatakse nii statistilistel eesmärkidel kui ka varundamise ja taaste jaoks.

(5) ISKE ohtude kataloog – infosüsteemide kolmeastmelise etalonturbe süsteemi ohtude kataloog.

(6) Turbeklass – andmete tähtsusest tulenev andmete nõutav turvalisuse tase, väljendatuna neljaastmelisel skaalal ning neljakomponendilisena, st kolme turvaosaklassi ühendina.

(7) Andmete töötlemine – andmete kogumine, salvestamine, korrastamine, säilitamine, muutmine, nende kohta päringute teostamine, nendest väljavõtete tegemine, andmete kasutamine, üleandmine, ühendamine,

sulgemine, kustutamine või hävitamine või mitu eeltoodud toimingut, sõltumata toimingute teostamise viisist või kasutatavatest vahenditest.

(8) Andmete omanik – isik, kes vastutab andmete loomise, klassifitseerimise, kasutamise, ligipääsude reguleerimise ja administreerimise eest terve elutsükli jooksul.

(9) Krüpteerimine – andmete teisendamine sellisele kujule, mida teistel on võimalik lugeda ainult vastava dekrüpteerimisvõtme olemasolu korral.

(10) Turvaintsident – mistahes kõrvalekalle süsteemide normaalse talitluse reeglitest.

(11) Varundamine – andmete koopia, mis on salvestatud algsest asukohast erinevasse asukohta.

§ 3. VASTUTUS

(1) Üldvastutus infoturbe tagamise eest on linnapeal.

(2) Infoturbealast tööd korraldab ja koordineerib ISKE koordinaator.

(3) Infoturbe meetmete rakendamist koordineerib vastutav isik.

(4) Iga struktuuriüksuse infoturbe eest vastutab selle üksuse juhataja.

(5) Konkreetsete turvameetmete rakendamise eest vastutajad määratakse linnapea käskkirjaga ja/või kajastuvad ametnike ametijuhendites.

(6) Kõik linnavalitsuse teenistujad ja töötajad vastutavad oma töövaldkonnas turbeeesmärkide saavutamise ja kehtestatud kordade täitmise eest.

(7) Vastutavate töötajate eemaloleku ajaks tuleb neile määrata ajutised asetäitjad.

(8) Logide ülevaatus tuleb sooritada vähemalt kord kuus.

(9) Väline audit tellitakse vastavalt vajadusele, aga mitte harvemini kui kord kolme aasta jooksul.

(10) Seadusandluse või turbeolukorra muutumisel tuleb linnapeal ja IT nõunikul – vastav infotehnoloogia spetsialist algatada infoturbe alusdokumentide ja meetmete muutmise protsess.

(11) Kolmeastmelisest etalonturbe süsteemi ISKE metoodikast lähtuvalt peab olemas olema linnavalitsuse infovarade spetsifikatsioon koos määratud turvaklassidega, mille alusel hinnatakse linnavalitsuse infovaradele asjakohaste ISKE turvameetmete rakendatust ja koostatakse edasine rakendamata meetmete rakendusplaan.

(12) Linnavalitsuse infovarade ja neile rakenduvate ISKE turvameetmete rakendatus vaadatakse läbi vähemalt kord aastas linnavalitsuse eelarve koostamisega koos või suuremate muutuste ja juhtumite korral. Läbivaatust koordineerib ISKE koordinaator. Läbivaatusel analüüsib ISKE koordinaator koostöös IT nõuniku – vastav infotehnoloogia spetsialist ja vastavate vastutusvaldkondade spetsialistidega ISKE rakendatuse tulemusi lähtudes ISKE ohtude kataloogist.

§ 4. INFOVARAD

(1) Varade üle peab arvestust vastutav isik.

(2) Linnavalitsuse infovarad ja nende turbeklassid kinnitatakse linnavalitsuse poolt.

(3) Infovarade kaitse tuleb tagada vähemalt ISKE meetme tasemel L.

§ 5. POLIITIKAD JA SUUNISED

(1) Personaliturve
1) Personali töölevõtul tuleb uuele töötajale tutvustada infoturvet reguleerivaid eeskirju.
2) Ametijuhendisse või töölepingusse tuleb lisada asjakohased turvanõuded.
3) Töötaja vabastamisel tuleb tagada viimase tööpäeva lõpuks kõikide tema valduses olevate varade ja pääsuvahendite tagastamine ning pääsuõiguste tühistamine.
4) Töötajaid tuleb teavitada neid puudutavate infoturbe meetmete muutustest ja turvaintsidentidest viivitamatult.
5) Töötajale peab olema tagatud infoturbealane koolitus.

(2) Üldturve:
1) üldturvet korraldab linnapea poolt määratud töötaja.
2) üldturbe regulatsiooni kehtestab linnavalitsus ja linnapea.
3) Ligipääs ruumidele tuleb tagada korraldatud tööalase vajaduse ja vastuse alusel. Võtmete arvu ja jagamise üle tuleb pidada kirjalikku arvestust.

4) Olulistes ruumides peab olema paigaldatud valvesignalisatsioon ning tagatud reageerimisvõimekus häirele.
5) Eraldi lukustatavas tööruumis tuleb viimasel väljujal sulgeda aknad ja lukustada uks.
6) Väline hoolde- ja remondipersonal lubada ruumidesse ainult koos saatjaga.

(3) Juhisdokumendid
Linnavalitsuse infovarade, turvameetmete loetelu, infosüsteemi kasutajate ja teenindajate õigused ning kohustused infosüsteemi töökindluse ja kasutusmugavuse tagamisel, infosüsteemi varundamise ning muud infoturvet reguleerivad korrad kehtestatakse linnavalitsuse poolt.

(4) Andmete ja dokumentide turve
1) Andmeturbe eesmärk on tagada andmete töötlemise vastavus kehtivatele õigusaktidele.
2) Kõigile andmetele on määratud omanik.
3) Vastutav isik korraldab andmete tehnilise haldamise ja administreerimise andmete omaniku eest ja vastavalt andmete omaniku poolt esitatud nõuetele infotehniliste vahenditega.
4) Asutustevaheline dokumentide ja andmekandjate üleandmine ning vastuvõtmine tuleb dokumenteerida.

(5) Pääsupoliitika
1) Juurdepääs infovaradele peab olema korraldatud tööalase vajaduse ja vastutuse alusel.
2) Pääsuparoole tuleb vahetada vähemalt kaks korda aastas.
3) Süsteemiparoolid peavad olema deponeeritud turvalises asukohas.

(6) Infovahetuse turve
1) Väljapoole linnavalitsuse ruume sattuvate töökohtade kõvaketastel olevad konfidentsiaalsed andmed peavad olema krüpteeritud.
2) Süsteemilogid tuleb säilitad vähemalt neli nädalat ja nende revisjon tuleb sooritada vähemalt kord kuus või vastavate turvaintsidentide korral.
3) Tuleb tagada kõigi tarbetute konfidentsiaalsete andmetega paberdokumentide ja füüsiliste andmekandjate hävitamine.
4) Töökohtade remonti saatmisel ja utiliseerimisel tuleb eelnevalt eemaldada füüsilised andmekandjad.
5) Töökohtades ja e-posti süsteemis peab olema rakendatud keskne viirustõrje.

(7) Varundamine
1) Iga töötaja vastutab tema kasutuses olevate andmete varukoopiate tegemise eest.
2) Vastutav isik vastutab keskse süsteemi varukoopia tegemise eest. Vähemalt kord aastas tuleb luua kõikidest andmetest varukoopia püsisäilituseks.

(8) Turvaintsidentide käsitlemine
1) Turvaintsidentide käsitlemise poliitika eesmärk on tagada turvaintsidentidest tuleneva kahju minimeerimine.
2) Turvaintsidentidest ja meetmete rakendamise mittevastavustest tuleb teavitada viivitamatult linnapead.
3) Infoturbe eest vastutav isik peab tagama intsidendile reageerimise, registreerimise ja hilisema analüüsimise.
4) Intsidentide analüüse kasutatakse alusmaterjalina turvameetmete rakendamise plaani koostamisel ja uuendamisel.

§ 6. INFOTURBEPOLIITIKA MUUTMINE

(1) Infoturbepoliitika värskendamine peab tagama selle pideva vastavuse organisatsiooni infoturbevajadusele.

(2) Infoturbepoliitika läbivaatus toimub kord aastas või peale suuremaid muutusi organisatsioonis, süsteemides või regulatsioonides või pärast tõsist intsidenti.

(3) Läbivaatust ja värskendamist korraldab ISKE koordinaator koos juhtkonna esindajatega.

(4) Muudatustest teavitatakse kõiki töötajaid.

§ 7. JÄRELEVALVE

(1) Järelevalvet infoturbepoliitika täitmise üle korraldab infoturbe eest vastutav isik.

(2) Infosüsteemide vastavust infoturbepoliitikale kontrollitakse sise- ja välisaudititega.

§ 8. Määrus jõustub 1. augustil 2010. a.