Väljaandja:	Rapla Vallavalitsus
Akti liik:	määrus
Teksti liik:	algtekst-terviktekst
Redaktsiooni jõustumise kp:	31.01.2020
Redaktsiooni kehtivuse lõpp:	Hetkel kehtiv
Avaldamismärge:	RT IV, 28.01.2020, 22

Rapla valla infoturbepoliitika

Vastu võetud 20.01.2020 nr 2

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

§ 1. Infoturbepoliitika rakendusala

(1) Rapla valla infoturbepoliitika sätestab Rapla vallavalitsuse kui ametiasutuse (edaspidi *ametiasutus*) ja selle hallatavate asutuste (edaspidi koos ka *asutus)*infoturbe eesmärgid ja nende saavutamise juhised, infoturbe korralduse ning peamiste turvameetmete rakendamise.

(2) Hallatavad asutused ei pea järgima korda osas, mis puudutab otseselt ametiasutuse siseseid toiminguid ja protsesse. Hallatava asutuse sisesed reeglid kehtestab hallatava asutuse juht.

(3) Hallatavad asutused ei pea rakendama infosüsteemide kolmeastmelise etalonturbe metoodikat asutuse infovarale.

(4) Infoturbepoliitikas arvestatakse ning põhimõtete elluviimiseks kavandatakse vastavad tegevused valdkondlikes valla õigusaktides.

(5) Infoturbepoliitika puudutab Rapla valla kui kohaliku omavalitsuse üksuse sisest suhtlust ning suhtlust riigiasutuste, teiste kohaliku omavalitsuse üksuste ja lepingupartneritega.

(6)Infoturbepoliitika hõlmab asutuse personali, infrastruktuuri, andmeid ja dokumentatsiooni, IT-riistvara, tarkvara ja sidesüsteeme.

(7) Infoturbepoliitikat on kohustatud järgima Rapla Vallavalitsuse kui täitevorgani liikmed ja Rapla Vallavolikogu liikmed, ametiasutuse ametnikud ja töötajad (edaspidi koos *teenistujad*), hallatavate asutuste töötajad, praktikandid ning Rapla vallavalitsuse ja hallatavate asutuste lepingupartnerid, kes on volitatud töötleja rollis.

§ 2. Mõisted

Infoturbepoliitika kirjeldamisel kasutatakse mõisteid järgmises tähenduses:
1) andmed – mis tahes viisil ja mis tahes infokandjale jäädvustatud või dokumenteeritud informatsioon ja kõikvõimalike IT-vahendite abil edastatav või töödeldav teave;
2) andmekogu – infosüsteemis töödeldavate korrastatud andmete kogum;
3) andmete käideldavus – teabe, IT-süsteemide kasutatavus, õigeaegne kättesaadavus ja kehtivus, inimeste ja protsesside teovõime ja kättesaadavus ajal, mil asutus seda vajab;
4) andmete konfidentsiaalsus – andmete salastatus, nende usalduslik käitlemine ja mitte avalikustamine, informatsioon on kättesaadav vaid volitatud isikutele;
5) andmete terviklus – andmete õigsus, puutumatus ja täielikkus, infovara lubamatute muudatuste puudumine; hõlmab ka info allika autentsust ja salgamatust;
6) andmevarundus – teatud ajahetkel varukoopia loomine varundamisele kuuluvatest andmetest, mis salvestatakse mõnele lisaandmekandjale. Andmevarunduse liigid on:
– täielik andmevarundus - varukoopia loomine kõigist varundamisele kuuluvatest andmetest;
– diferentseeritud andmevarundus – varukoopia tegemine ainult sellistest failidest, mis on võrreldes viimase täieliku andmevarundusega muutunud;
– inkrementaalne andmevarundus – vastupidiselt täielikule andmevarundusele varukoopia tegemine ainult sellistest failidest, mis on võrreldes viimase andmevarundusega muutunud.
7) infosüsteem – andmeid töötlev, salvestav või edastav tehniline süsteem koos tema normaalseks talitluseks vajalike vahendite, ressursside ja protsessidega;

8) infosüsteemide kolmeastmeline etalonturve (edaspidi *ISKE*) − infoturbe metoodika, mida rakendatakse infovarale ja mis sisaldab juhised ning turvameetmete kataloogi, kuidas korraldada infoturbe haldust, määrata infovarade turbevajadust ja turvameetmeid;
9) infoturbe haldus – protsess, mida kasutatakse infovara konfidentsiaalsuse, tervikluse ja käideldavuse asjakohaste tasemete saavutamiseks ja säilitamiseks. Infoturbe halduse põhifunktsioonide hulka kuuluvad strateegilise infoturbepoliitika (põhimõtete) ja selle rakendamise kava koostamine, infoturbe organisatsiooni loomine, riskihaldus ja infoturbe käigus hoidmine;
10) infoturve ehk andmekaitse – turvameetmete loomise, valimise ja rakendamise protsesside kogum, mis tagab andmete tervikluse, käideldavuse ja konfidentsiaalsuse;
11) infovara – mistahes kujul talletatud andmed ja informatsioon, mis on asutusele väärtuslik ja mida asutus kasutab oma põhimääruses ettenähtud ülesannete täitmiseks ning asutuse omandis olevad infotöötlusvahendid, rakendused ja taristu, mis tagavad asutusele informatsiooni nõuetekohase töötlemise;
12) kasutaja – ametis olev ametnik või töötaja;
13) kasutajatugi – vallavalitsuse IT-spetsialist või võlaõigusliku lepingu olemasolu korral lepingus märgitud kontaktisik;
14) krüpteerimine – andmetele kõrvaliste isikute jaoks loetamatu kuju andmine;
15) privaatsus – üksikisiku eraellu või juriidilise isiku ärisaladusse tungimise või tema kohta kogutud andmete kasutamise välistamine väljaspool ametiülesannete täitmist;
16) 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;
17) turvameetmed – organisatoorsed toimingud ja vahendid, tehnilised protsessid ja tehniliste vahendite rakendamine andmete ja infosüsteemide turvalisuse saavutamiseks ja säilitamiseks;
18) vahendid – infrastruktuur (näiteks hooned, ruumid, kaablid, võrguühendus), arvutid (näiteks lauaarvutid, sülearvutid, tahvelarvutid), lisaseadmed (näiteks printerid), andmekandjad (näiteks serverid, mälupulgad, CD-d, DVD-d) jms;
19) varundamine – andmete kopeerimine, mis tähendab nende salvestamist algsest asukohast erinevasse asukohta.

§ 3. Põhimõtted

(1) Infosüsteemide ja infovarade turvalisus tagatakse nende varade käideldavuse, tervikluse ja konfidentsiaalsuse säilitamisel nõutaval või kokkulepitud tasemel (ISKE auditis).

(2) Käideldavuse, tervikluse ja konfidentsiaalsuse säilitamine nõutaval või kokkulepitud tasemel tagatakse turvameetmete rakendamisega ulatuses, mis tagab ohtude realiseerumisel Rapla valla kui kohaliku omavalitsuse üksuse ülesannete tavapärase ja katkestusteta täitmise.

(3) Turvameetmed jagunevad organisatsioonilisteks, füüsilisteks ja infotehnilisteks. Turvameetmed peavad olema majanduslikult õigustatud ning nende negatiivne mõju asutuse tegevusele ja teenistujate tööle peab olema tasakaalus meetmete rakendamata jätmisel tekkida võiva kahjuga.

(4) Turvameetmete pideva asjakohasuse tagamiseks on vajalik turvameetmete hooldus, regulatsioonide perioodilised läbivaatused, töökeskkonna igapäevane seire, infoturbe perioodiline vastavusekontroll, muudatustele reageerimine ja infoturbeintsidentide käsitlus.

(5) Kõiki infosüsteemi muudatusi tuleb enne nende läbiviimist kaaluda infoturbe seisukohast. Muutunud nõuete või uute ohtude korral tuleb turvameetmed ümber hinnata.

§ 4. Eesmärgid

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

(2) Infoturbe eesmärgiks on:
1) kaitsta andmeid ohtude eest;
2) tagada andmete väärtuste ja omaduste säilimine;
3) tagada talituse jätkuvus;
4) minimeerida talitusriski;
5) maksimeerida investeeringute tasuvust;
6) tagada vastavus õigusaktidele;
7) säilitada asutuse kuvand.

(3)Infoturbe tähtsus tuleneb andmete tähendusest ja väärtusest. Andmete tähendus ja väärtus määratakse ISKE metoodika alusel.

§ 5. Turvariskide hindamise mõisted

Turvariskide hindamisel kasutatakse mõisteid järgmises tähenduses:
1) oht – olukord, mis võib kahjustada infovarasid ning võib peituda infrastruktuuris, tehnoloogias, inimeste turbeteadlikkuses või asutuse töökorralduses.

Ohuallikaks võivad olla:
a) puudused infrastruktuuris – ebapiisav kaitse füüsiliste ohtude eest (näiteks kuum, külm, elektrikatkestus) või turbe füüsiliste meetmete osaline rakendamine;
b) puudused infotehnoloogias – süsteemide või seadmete tõrked (näiteks serveririke või võrguühenduse katkestus), seadmete paigutus, süsteemide jõudlus või ülepingutatud turvameetmed;
c) puudused inimeste töös − vead, mida inimesed teevad turvanõuete järgimisel (näiteks antakse edasi ligipääsuõigusi või taotletakse tarbetuid ligipääsuõigusi, ei järgita töö- ja eraasjade lahususe põhimõtet);
d) 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 või arvutisse on paigaldatud volitamata tarkvara;
e) turvaründed;
2) nõrkus – infovara omadus, mis laseb ohul realiseeruda;
3) risk – tõenäosus, et oht kasutab ära nõrkuse ja tekitab infovarale kahju;
4) jääkrisk – risk, mida on mõistlik aktsepteerida;
5) turvaintsident – mistahes kõrvalekalle infosüsteemi normaalse talitluse reeglitest.

§ 6. Turvariskide vältimise meetod

Riskide minimeerimiseks vastuvõetavale tasemele võetakse asutuses kasutusele järgmised meetmed:
1) füüsilised meetmed ruumidele (näiteks uste, akende, seinte ja lukkudega seotud abinõud);
2) organisatsioonilised meetmed teenistujatele (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).

§ 7. Riskihaldus

(1) Asutuste 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 või peab kinnitama meetme täitmata jätmisega tekkinud jääkriski aktsepteerimise.

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

§ 8. Turvaintsidentide haldus

(1) Turvaintsidendist või selle ohust peab teenistuja koheselt teavitama ametiasutuse andmekaitsespetsialisti ja IT-spetsialisti.

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

(3) Turvaintsidentide haldus sätestatakse turvaintsidendi käsitlemise korras.

§ 9. Infovarade ligipääsu reguleerimine

(1) Ligipääs infovaradele tagatakse vaid volitatud kasutajatele autoriseerimismeetoditega. Kõik õnnestunud ja ebaõnnestunud autoriseerimiskatsed registreeritakse automaatselt.

(2) Pääsuõiguste jagamisel lähtutakse ametialase teadmisvajaduse põhimõttest. Pääsuõigused taotleb vahetu juht ja kinnitab pädev töötaja (IT-spetsialist ja/või andmekaitsespetsialist).

(3) Pääsuõiguste taotlemisel ja seadistamisel lähtutakse võimalusel kohustuste lahususe printsiibist, kus pääsuõiguste taotleja ei saa olla pääsuõiguste seadistaja. Taotletud, kinnitatud ning seadistatud pääsuõigused dokumenteeritakse.

(4) Pääsuõiguste jagajad võtavad kasutusele protseduurid, reeglid või muud mehhanismid, mis tagavad pääsuõiguste tühistamise, kui teenistuja kaotab usalduse või tema töösuhe lõpeb.

(5) Infovarade kasutajad tuvastatakse, kasutades asjakohaseid autentimismehhanisme. Uute infosüsteemide projekteerimisel eelistatakse Eesti ID-kaardi põhist autentimist.

(6) Reeglid, mille järgi valitakse salasõna, selle kehtivus ja muud parameetrid, on kehtestatud vallavanema käskkirjaga infosüsteemide kasutamise korras.

(7) Andmete töötlemiseks asutustes kasutatakse vaid asutuse kinnitatud riist- ja tarkvarastandardile vastavaid infotehnoloogilisi vahendeid. Asutuse sisevõrku ei tohi ühendada asutusele mittekuuluvaid seadmeid.

§ 10. Krüpteerimine ja sõnumiautentimine

(1) Asutusesiseseks kasutamiseks mõeldud teabe edastamisel välisvõrkude vahendusel peab see olema krüpteeritud.

(2) Välisvõrkude vahendusel edastatud teabe sisestamisel andmekogudesse kasutatakse kaheastmelise autentimise meetodeid.

(3) Krüpteerimise ja sõnumiautentimise detailid sätestatakse infosüsteemide juhendmaterjalides. Nende puudumisel kasutatakse ID-kaardil põhinevat krüpteerimist ja ID-kaardi digitaalallkirjal põhinevat sõnumiautentimist.

§ 11. Kontrolljäljed

(1) Toimingute või sündmuste ajaloo väljaselgitatavuse tagamiseks salvestatakse ja säilitatakse infovarade haldamise ja kasutamisega seotud kontrolljäljed ehk logid. Toimingute ja sündmuste nimekiri, mille kohta kontrolljälgi salvestatakse ja säilitatakse ning kontrolljälgede säilitamise tähtaeg tuleneb seadusest, infovaradele määratud turvaklassist ja sellele vastavatest turvameetmetest.

(2) Kontrolljälg peab sisaldama vähemalt teostaja identiteeti, juhtumit ja toimumise aega.

(3) Kontrolljälgede salvestamisel ja säilitamisel peab olema tagatud nende vältimatus, käideldavus, terviklus ja konfidentsiaalsus.

§ 12. Viirusetõrje

Kõikidele infosüsteemidele ja edastatavatele andmetele rakendatakse viirusetõrjet, mille andmebaase uuendatakse perioodiliselt.

§ 13. Infosüsteemide kasutusele võtmine ja muudatused

(1) Uued infosüsteemid või olemasolevate infosüsteemide olulised muudatused testitakse enne kasutusele võtmist. Testid peavad sisaldama infoturbe regressiooniteste.

(2) Enne uute infosüsteemide kasutusele võtmist rakendatakse neile vajalikud turvameetmed.

(3) Kõiki infosüsteemi muudatusi tuleb enne nende tegemist kaaluda infoturbe seisukohast. Turvameetmed tuleb viia vastavusse muutunud nõuete või uute ohtudega.

§ 14. Varundamine

(1) Nii andmekogudes sisalduvad kui ka muud esmatähtsad andmed varundatakse regulaarselt, et oleksid tagatud seadustest ning tööprotsessidest tulenevad käideldavuse ja tervikluse nõuded. Varundatud andmete taastamist testitakse regulaarselt.

(2) Andmekogude varundusnõuded kehtestatakse igale andmekogule eraldi. Muude andmete varundusnõuded kehtestab asutuse juht.

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

(4) Varundatud andmete hoidmisel rakendatakse ISKE turvameetmeid, lähtudes varundatud andmete maksimaalsest turvaklassist.

§ 15. Turvastandardid ja ISKE

(1) Andmekogudega seotud asjakohaste turvameetmete määramisel lähtutakse ISKE rakendusjuhendis toodud metoodikast ning ohtude ja turvameetmete kataloogist.

(2) Vajadusel rakendatakse lisaks etalonturvameetmetele ka muid turvameetmeid, mis tagavad infovarade käideldavuse, tervikluse ja konfidentsiaalsuse nõutaval tasemel.

(3) Andmekogudega seotud turvameetmete rakendamisel järgitakse auditeeritavuse printsiipi. Rakendatavad turvameetmed peavad olema põhjendatud ja dokumenteeritud selliselt, et hiljem oleks võimalik hinnata nende vajalikkust ning asjakohasust.

(4) ISKE rakendusjuhendi ja teiste juhendmaterjalide tõlgendamisel lähtutakse mõistlikkuse printsiibist ja arvestatakse infoturbe üldist eesmärki.

(5) Dokumenteerida tuleb nii ISKE rakendusjuhendi tõlgendused kui ka põhjendused, kui ISKE turvameetmete kataloogis sätestatud turvameetmeid ei ole rakendatud.

§ 16. Füüsiline turve

(1) Ligipääs ruumidele tagatakse töövajaduse ja vastutuse alusel. Ruumide avamiseks välja antud ning võtmete üldarvu kohta peab arvestust Rapla vallavalitsuse personalispetsialist ringkäigulehe alusel.

(2) Töövälisel ajal valvatakse hooneid ja ruume elektrooniliselt. Esmatähtsad ruumid on ka tööajal lukustatud.

§ 17. Konfidentsiaalsuskohustus

(1) Konfidentsiaalsuskohustus kehtib konfidentsiaalse teabe kohta ega sõltu isiku ametikohast ja töötegemise asukohast. Konfidentsiaalsuskohustus kohaldub ka neile teenistujatele ja praktikantidele, kellel puuduvad otsesed infovara kasutamise volitused.

(2) Kui töötaja või praktikant tegutseb lepingu alusel, peab leping sisaldama konfidentsiaalsuskohustuse sätteid.

(3) Kui lepingulisi kohustusi täidab teine organisatsioon või asutus (kolmas osapool), peab asutuse ja kolmanda poole vahel sõlmitud leping sisaldama konfidentsiaalsuskohustuse sätteid. Pooled allkirjastavad lepingu enne, kui lepingu täitjale võimaldatakse juurdepääs infovarale.

§ 18. Teenistujad

(1) Teenistuja infoturbega seotud õigused, kohustused ja vastutus määratakse ametijuhendis, infoturbe juhendites ja/või muudes asjakohastes eeskirjades ja/või kordades.

(2) Enne teenistuja tööle asumist tutvustatakse talle asutuse infoturbe põhimõtteid ja -reegleid. Reeglitega tutvumise ja nendest arusaamise kohta annab teenistuja allkirja.

(3) Teenistujaid teavitatakse nende töövaldkonda puudutavatest infoturbe meetodite muutustest ja turvaintsidentidest viivitamatult.

(4) Infoturbe tagamiseks organisatsioonis korraldatakse teenistujatele regulaarselt turvateadlikkuse koolitusi. Infoturbe eest vastutava(te)le isiku(te)le võimaldatakse erialaseid täienduskoolitusi.

(5) Teenistussuhte lõppemisel tagastab teenistuja viimasel tööpäeval tööandjale kõik varad ja pääsuvahendid, mis olid tema valduses. Teenistuja ligipääsuõigused infosüsteemidele tühistatakse.

§ 19. Andmete ja dokumentide turve

(1) Andmeid töödeldakse kehtivate õigusaktide kohaselt.

(2) Kõigile andmetele määratakse omanik (ISKE auditis).

(3) Andmete tehnohaldamist ja administreerimist infotehnoloogiliste vahenditega korraldab andmete omaniku volitatud isik (teenuse pakkuja) turvanõuete kohaselt.

(4) Asutustevaheline dokumentide ja andmekandjate üleandmine ja vastuvõtmine dokumenteeritakse.

§ 20. Infoturbe põhimõtetele tuginevate õigusaktide kehtestamise õigus

Vajadusel võib infoturbe põhimõtete rakendamiseks vajalikke nõudeid ja meetmeid kehtestada asutuse töökorralduse reeglite või asutuse juhi käskkirjaga. Nõuded ja meetmed peavad tuginema infoturbe põhimõtetele ja olema kooskõlas õigusaktidega.

§ 21. Infoturbepoliitika muutmine

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

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

Meelis Mägi
vallavanem

Ülle Eesik-Pärn
vallasekretär