TORI VALLAVALITSUS

VALLAVANEMA KÄSKKIRI

Sindi 21. jaanuar 2020 nr 13-2/4

Tori Vallavalitsuse infoturbe poliitika kinnitamine

Kohaliku omavalitsuse korralduse seaduse § 50 lõike 1 punkti 3 alusel ja arvestades Vabariigi Valitsuse 20.12.2007 määrust nr 252 „Infosüsteemide turvameetmete süsteem“, Riigi Infosüsteemide Arenduskeskuse poolt koostatud „Infosüsteemide kolmeastmelise etalonturbesüsteem ISKE rakendusjuhendit“ kinnitan Tori Vallavalitsuse infoturbe poliitika järgmiselt:

I Sissejuhatus

1. Käesolev poliitika määratleb infoturbe strateegia üldalused ja sellega on kohustatud tutvuma Tori vallavalitsuse (edaspidi vallavalitsuse) ametnikud, abi- ja koosseisuvälised teenistujad, töövõtu- või muu lepingu alusel teenust osutavad isikud ja kõik teised isikud, kes osalevad valla töös (edaspidi töötaja).
2. Ülevallalise infoturbe poliitika eesmärk on deklareerida valdkonnaga tegelemise vajalikkust asutuses ning kirjeldada organisatsiooni üldist, strateegilist lähenemisviisi infoturbe tagamisel.

II Deklaratsioon

3. Infovarad on tähtsad vallavalitsuse tõhusaks ja toimivaks igapäevaseks tegevuseks ning neid tuleb kasutada ainult määratud otstarbel. Valla üleorganisatsiooniline poliitika on anda juurdepääs infovaradele ainult tõendatud teadmisvajaduse alusel ja keelata juurdepääs kõigil teistel. Tori Vallavalitsus peab vajalikuks infoturbega tegeleda ning teeb selle kõigile töötajatele kohustuslikuks.

III Mõisted

4. Valla infosüsteemide varad (edaspidi infovara) on käesoleva poliitika tähenduses vallavalitsuses kasutusel olevad infotehnoloogilised vahendid ja viimaste abil töödeldavad andmed. Infotehnoloogilised vahendid on riist- ja tarkvara ning andmesideseadmed.
5. Andmed võivad olla mis tahes viisil ja mis tahes andmekandjale jäädvustatud või dokumenteeritud teave ning kõikvõimalike (infotehnoloogiliste) vahendite abil edastatav või töödeldav teave.
6. Infoturve ehk andmekaitse tähendab andmete kolme põhiomaduse – tervikluse, käideldavuse ja konfidentsiaalsuse tagamist, kus:
    6.1. *käideldavus* tähendab informatsiooni kasutuskõlblikkust ja õigeaegset kättesaadavust volitatud isikule;
    6.1. *terviklus* tähendab, et info pärineb autentsest allikast ning seda ei ole volitamatult muudetud ega kustutatud;

6.2. *konfidentsiaalsus* tähendab, et informatsioon on kättesaadav vaid volitatud isikutele.

7. Infoturbe haldus on protsess, mida kasutatakse infovara konfidentsiaalsuse, tervikluse ja käideldavuse asjakohaste tasemete saavutamiseks ja säilitamiseks. Infoturbe halduse põhifunktsioonide hulka kuuluvad strateegiline infoturbe poliitika, riskihaldus ja infoturbe käigushoidmine.

8. Konfidentsiaalseks ehk avaldamisele mitte kuuluvaks teabeks peetakse selliseid andmeid, millele on juurdepääs lepingu või seaduse alusel või mis on mõnel muul alusel kuulutatud mitteavalikuks.

9. Infoturbeintsidendiks loetakse kõiki reaalse või potentsiaalse kahju juhtumeid, mis võivad ohustada või halvata infovara turvalisust, põhjustades nende käideldavuse (töökindlus), tervikluse (andmete õigsuse ja muutumatuse) või konfidentsiaalsuse (andmete salastatuse) kao. Infoturbeintsidentideks loetakse muuhulgas ka toimingud, mis ei ole infoturbe valdkonda reguleerivate õigusaktidega kooskõlas.

10. Infosüsteemide kolmeastmelise turvameetmete süsteemi mõistet kasutatakse käesolevas poliitikas Vabariigi Valitsuse 20. detsembri 2007. a määruses nr 252 „Infosüsteemide turvameetmete süsteem“ defineeritud tähenduses. Infovarade turvaklassid määratakse ja nendele vastavad turvameetmed valitakse töödeldavate andmete koosseisu alusel ja nimetatud määruses kirjeldatud infosüsteemide kolmeastmelise etalonturbe (edaspidi ISKE) metoodikat järgides.

11. Turvaklassiks loetakse ISKE rakendusjuhendi alusel määratud infovara turvaklassi.

IV Infoturbe eesmärk

12. Tori vallavalitsus täidab ametiasutusena seadusest tulenevaid ülesandeid. Valla infoturbe eesmärkideks on tagada:

12.1. valla igapäevane asjaajamine ja infovahetus, kus põhieesmärgiks on töötaja ootustele vastava, stabiilse, turvalise ja töökindla töökeskkonna tagamine ja talitlusvõime säilitamine;

12.2. valla ja kodaniku vaheline infovahetus, kus eesmärgiks on avaliku info kättesaadavus infovajajale ning avalike teenuste kiire ja tulemuslik osutamine;

12.3. vallale töötlemiseks või hoidmiseks antud andmete konfidentsiaalsus ja terviklus;

12.4. infosüsteemide ja andmekogude pidamine ning arendamine vastavalt Eesti Vabariigis kehtivatest õigusaktidest tulenevatele infoturbenõuetele.

13. Infoturbe eesmärkide saavutamiseks tuleb tagada infovarade kolm infoturbe osaeesmärki:

13.1. *Käideldavus* – kuna asutuses on kesksel kohal tegevuskriitilisi infosüsteeme ja ulatuslikke tööülesandeid, mida täidetakse infotehnoloogia abil, on oluline kehtestada ja täita teenustasemete kokkuleppeid ning tagada infosüsteemide talitluspidevus kriisiolukorras vastavalt talitluspidevuse poliitikas sätestatule;

13.2. *Terviklus* – töödeldav informatsioon peab olema usaldatav, vigu peab vältima tarkvara terve elutsükli jooksul ja andmete tõepärasust peab regulaarselt kontrollima. Avaliku teabe seaduse või muu õigusakti alusel töödeldava andmekogu või infosüsteemi täielik kustutamine peab olema välistatud;

13.3. *Konfidentsiaalsus* – kriitilistel aladel peab konfidentsiaalse teabe kaitse olema selgelt määratletud ja vastama asjakohastele (seadusest tulenevatele) nõuetele. Tagada tuleb ka üldiseks kasutamiseks mõeldud teabele avalikkuse ja igaühe juurdepääsu võimalus ning asutusesiseseks kasutamiseks määratud informatsiooni salastatus. Valla eesmärk on anda juurdepääs informatsioonile ainult tõendatud teadmisvajaduse alusel ja keelata juurdepääs kõigil teistel.

V Infoturbe organisatsioon ja juhtimine

14. Infoturbe toimimiseks on vajalik lisaks eesmärkide teadvustamisele, et asutuses oleks kindlalt määratletud turvaalased rollid ja vastutused. Infoturve on organisatsiooni kollektiivne tegevus ja kõikide töötajate kohustus. Iga töötaja peab teadma, milles seisneb tema panus infoturbesse.

15. Valla infoturbe infrastruktuur peab tagama optimaalsed kulutused asutuse turvanõuete täitmiseks ja asutuse varade kaitseks.

16. Infoturbealane vastutus jaguneb üldiseks ja konkreetseks vastutuseks:

16.1. Üldine infoturbealane vastutus on asutuse töötajal ja seisneb antud valdkonda reguleerivate kordade järgimises ning infoturbeintsidentidest teavitamises.

16.2. Konkreetne, st rolli- või ametikohapõhine vastutus järgib organisatsiooni struktuurilist ülesehitust, üldist töökorraldust, tegevusvaldkondi ja kehtivaid delegeerimispõhimõtteid. Kõige kõrgemal tasemel on vastutajaks Tori Vallavalitsus, seejärel kandub vastutus edasi osakondade tasemele, kuni iga töötaja individuaalse turvaalase vastutuseni välja.

17. Infoturbealased otsused teeb IT-juht koostöös vallavanemaga. Infovara valdajana on IT-juht kohustus täita vähemalt järgmised infoturbealased ülesanded:

17.1. määratleda valdkonna tähtsamad eesmärgid, hinnata peamisi riske, kinnitada infovaradele määratud turvaklassid;

17.2. kooskõlastada ja kinnitada tunnustatud standarditega kooskõlas olev üleorganisatsioonilise infoturbe strateegia ning toetada ja hinnata selle rakendamist;

17.3. kooskõlastada ja kinnitada muu antud valdkonda puudutav regulatsioon, mis kehtib kogu vallas;

17.4. osaleda infoturbe olulisusest teavitamises;

17.5. määratleda infovarale kindlad omanikud;

17.6. tellida sõltumatuid hinnanguid infoturbe valdkonnale;

17.7. aktsepteerida jääkriskid kooskõlastatult vallavanemaga.

18. Valla infoturbe koordineerimiseks ja oluliste turvaalaste otsuste tegemiseks on ametis IT-juht. IT-juhi ülesanneteks on:

18.1. infoturbealase aruandluse ja statistika läbivaatamine;

18.2. suurematele infoturbealastele probleemidele lahenduste leidmine;

18.3. infoturbealaste prioriteetide paika panemine;

18.4. infoturbealaste ostuste tegemine oma volituste piires.

19. Infovara omanik vastutab infosüsteemi vastavuse eest organisatsiooni vajadusele. Infovara omanikul on täita vähemalt järgmised infoturbealased ülesanded:

19.1. määrata tema kontrolli all oleva informatsiooni või infotöötlussüsteemide turvaklass vastavalt ISKE määrusele ja tagada turvaklassi määramise aluste säilimine kirjalikult taasesitatavas vormis ning turvaklassi kinnitamine IT-juhi poolt;

19.2. aktsepteerida infovarale rakendatavad turvanõuded ning jääkrisk;

19.3. defineerida rakendustarkvara kasutajaõigused ning kasutajaõiguste andmise ja ära võtmise alused;

19.4. vastutada infovara kasutamise õiguspärasuse eest koostades infovara kasutujuhendid, volitades infovarale ainult õigusaktides lubatud kasutajad ja kontrollides volitatud kasutajate tegevust.

20. Infovara kasutaja (edaspidi kasutaja) on töötaja, kellele infovara omanik on volitanud infovara kasutamise õigused. Kasutajate kohustus on toetada ja järgida asutuses kehtivaid kordasid, mis reguleerivad infovarade kasutamist ja kaitset.

21. Asutuse infoturbe eest vastutav isik täidab oma vastutuspiirkonnas infoturbealaseid kohustusi lähtuvalt käesolevast poliitikast või muust antud valdkonda reguleerivast õigusaktist ning kohustub täitma vähemalt järgmisi infoturbealaseid ülesandeid:

21.1. mõista asutuse infoturbealaseid vajadusi;

21.2. korraldada ISKE turvameetmete, mis ei kuulu IT valdkonda, rakendamine asutuses, selleks konsulteerib ta vajadusel IT-juhiga ja juhindub tema poolt antud soovitustest;
21.3. teavitada kõiki valla töötajaid valdkonna olulisusest ning tagab, et kõik asutuse töötajad oleksid oma infoturbealasest vastutusest teadlikud;
21.4. jälgida, et asutuses rakendatavad turvameetmed on kooskõlas kehtivate poliitikate, standardite, eeskirjade ja kordadega;
21.5. korraldada asutuse töö selliselt, et uue töötaja andmed on edastatud asutuse personali eest vastutavale isikule enne, kui talle tellitakse infovara kasutusõigused;
21.6. korraldada asutuse töö selliselt, et infovara kasutaja töökohustuste muutumisest või töösuhte lõppemisest teavitatakse koheselt infovara kasutusõiguste andjat, tagamaks kasutajaõiguste õigeaegse muutmise või ära võtmise;
21.7. korraldada vajadusel infoturbealaseid koolitusi;
21.8. kontrollida, et asutuses täidetaks infoturbealaseid poliitikaid, standardeid, eeskirju ja kordasid ning ei esineks infovara volitamata kasutamist.

22. Tori vallavalitsuse IT-juht on infoturbe valdkonda koordineeriv isik, kes nõustab infovara omanikke, kasutajaid ja administraatoreid infoturvet puudutavates küsimustes ning koordineerib antud valdkonna töid läbi järgmiste tegevuste:
22.1. vastutab infoturbega seotud ülesannete täitmise eest ning tagab infoturvet reguleerivate juhiste olemasolu, elluviimise ja ajakohastamise;
22.2. nõustab töötajaid organisatoorsete ja füüsiliste infoturbemeetmete rakendamise osas;
22.3. teeb oma ülesannete täitmisel muuhulgas koostööd töötajatega, isikuandmete töötlemise eest vastutava isikuga ning riigi andmekogudele kohustusliku infosüsteemide turvameetmete süsteemi (ISKE) rakendajaga;
22.4. osaleb infosüsteemide arendusprojektides ning nõustab infoturbe riskide hindamisel, uute turvameetmete loomisel või olemasolevate parendamisel;
22.5. juurutab asutuses turvaintsidentide haldamise korra ning teavitab viivitamatult intsidentide käsitlemise osakonda (CERT-EE) olulistest turvaintsidentidest nende nõuete järgi, mis on toodud Vabariigi Valitsuse 20. detsembri 2007. a määrusega nr 252 ”Infosüsteemi turvameetmete süsteemi kehtestamine” kehtestatud rakendusjuhendis.
22.6. korraldab infosüsteemide valmisoleku hädaolukorraks ning taasteplaani koostamise;
22.7. teavitab töötajaid turvareeglitest, nõustab neid infoturbealaselt ning vajadusel korraldab asutuse töötajatele koolitusi üldise turvateadlikkuse tõstmiseks;
22.8. Kontrollimisel, tähelepanekute ja järelduste tegemisel, soovituste andmisel ning tulemustest teavitamisel on IT-juht sõltumatu ja kontrollitava suhtes objektiivne;
22.9. IT-juht teavitab asutuse juhti asjaolust, mis ohustab tema objektiivsust tööülesande täitmisel.

23. Administraator on käesoleva poliitika mõistes isik, kes teostab infovarade haldust, tagades nendega töötamiseks vajalikud tingimused. Administraatori ülesandeid täidab teenuse pakkuja töötaja või lepinguga määratud füüsiline või juriidiline isik. Juriidilise isiku puhul peab lepingus olema märgitud füüsiline isik, kes teostab infovara haldust. Administraator vastutab valla infoturbe poliitika põhjal koostatud rakenduskava elluviimise eest ja täidab turvaalast funktsiooni vastavalt oma ametijuhendile, lepingule või muule kehtivale infoturbealasele regulatsioonile. Turvapoliitika elluviimine seisneb turvameetmete kavandamises, planeerimises, loomises, evitamises, haldamises, administreerimises vms.

VI Riskihaldus

24. Vallavalitsuse jäme riskihaldus põhineb ISKE kolmastmelise etalonturbe metoodikal. ISKE määrab ära minimaalsed turvameetmed, mida tuleb rakendada infovaradele ettenähtud turvataseme saavutamiseks ja säilitamiseks.

25. Riski vähendamiseks rakendatakse ISKE turvameetmeid vastavalt infovaradele määratud turvaklassile ja ISKE rakendusjuhendile.
26. Kui mõnda ISKE turvameedet ei ole võimalik või otstarbekas täita peab leidma alternatiivsed meetmed riski vähendamiseks või peab vallavanem kinnitama meetme täitmata jätmisega tekkinud jääkriski aktsepteerimise.
27. Kui infosüsteemi omanik leiab, et ISKE- põhisest riskianalüüsist ei piisa, koostatakse lisaks detailne riskianalüüs, kus vaadatakse eraldi iga infovarale mõjuvat ohtu, hinnatakse ohu realiseerumise tõenäosust, määratakse suuremad riskid ja võetakse vajadusel kasutusele spetsiifilised meetmed nende vähendamiseks.

VII Infoturbe protsess

28. Turvameetmete pideva asjakohasuse tagamiseks on vajalik turvameetmete hooldus, regulatsioonide perioodilised läbivaatused, infoturbe perioodiline vastavusekontroll, muudatustele reageerimine ja infoturbeintsidentide käsitlus.
29. Kõiki infosüsteemi muudatusi tuleb enne nende läbiviimist kaaluda infoturbe seisukohast. Muutunud nõuete või uute ohtude korral tuleb turvameetmed ümber hinnata.
30. Tori Vallavalitsuse jaoks on väga oluline pidev turvanõuete vastavuse kontroll, et tagada turvanõuete täitmine ning turvanõuete vastavus tegelikule olukorrale.
31. Väline turvanõuete audit tellitakse vastavalt vajadusele, kuid mitte harvemini kui Vabariigi Valitsuse 20. detsembri 2007. a määruses nr 252 „Infosüsteemide turvameetmete süsteem“ kehtestatud korras.

VIII Infoturbeintsident ja kontrolljäljed

32. Infoturbeintsidendist ja selle ohust peab iga töötaja võimalikult kiiresti teavitama IT-juhti või teda asendavat isikut.
33. Infoturbeintsidentide lahendamine toimub IT-juhi poolt selleks määratud isiku koordineerimisel, kes rakendab vastavalt tekkinud olukorrale asjakohast reageerimist. Infoturbeintsidentide avastamise üheks eelduseks on jälitatavuse toimivus.
34. Jälitatavuse tagamiseks salvestatakse ja säilitatakse infovarade haldamise ja kasutamisega seotud toimingute teostamise kohta kontrolljälgi (logisid). Toimingute liik, mille teostamise kohta kontrolljälgi salvestatakse ja säilitatakse, samuti kontrolljälgede säilitamise tähtaeg, kehtestatakse vastavalt seaduses sätestatud nõuetele ning infovaradele määratud turvaklassile ja sellele vastavatele ISKE rakendusjuhendis sisalduvatele turvameetmetele.
    34.1. Kontrolljäljed peavad sisaldama vähemalt toimingu teostaja nime, toimingu liiki ja toimingu teostamise aega.
    34.2. Kontrolljälgede salvestamisel ja säilitamisel peab olema tagatud nende vältimatus, käideldavus, terviklus ja konfidentsiaalsus.
35. Infoturbeintsidendi lahendamiseks on IT-juhil või selleks määratud isikul juurdepääsuõigus sellistele kontrolljälgedele ja muule arvutivõrgus olevale informatsioonile, mis on situatsiooni lahendamiseks vajalik, välja arvatud sõnumisaladusena käsitlevale informatsioonile.
36. Intsidendi lahendamise käigus kogutud informatsioon dokumenteeritakse ja analüüsitakse eesmärgiga vältida sarnaste intsidentide aset leidmist tulevikus ning otsustamaks täiendavate turvameetmete rakendamise vajaduse üle.
37. Kui turvaintsidendi lahendamise käigus avastatakse kuriteo, väärteo- või distsiplinaarsüüteo või töölepingu rikkumise tunnused, antakse juhtum edasi menetlemiseks vastava menetluse läbiviimise õigust omavale asutusele või isikule.

IX Konfidentsiaalkohustuse nõue

38. Konfidentsiaalkohustuse nõue kehtib konfidentsiaalse teabe kohta ja on sõltumatu isikute ametiseisundist või füüsilisest töökohast ning kohaldub ka neile töötajatele, kellel puuduvad otsesed infovara kasutamise volitused.

39. Töötaja, kes puutub tööülesannete täitmisel või töö käigus juhuslikult kokku konfidentsiaalsete andmetega, kohustub minimaalselt:

39.1. mitte avalikustama temale teatavaks saanud konfidentsiaalset informatsiooni, välja arvatud kui see on seadusega kohustuslik või vajalik tööülesannete täitmiseks;

39.2. järgima kehtivaid andmekaitset puudutavaid õigusakte ja kordasid;

39.3. täitma konfidentsiaalkohustuse nõudeid nii töösuhte ajal kui ka peale selle lõppemist.

40. Kui töötaja tegutseb töövõtu või muu lepingu alusel, peab vastav leping sisaldama käesoleva korra punktides 39.1-39.3 ette nähtud konfidentsiaalkohustuse nõuete sätteid.

41. Kui lepinguliste kohustuste täitjaks on teine organisatsioon või asutus, näiteks koostöös kolmandate osapooltega, peab:

41.1. vallavalitsuse ja kolmanda osapoole vahel olema sõlmitud leping, mille pooled allkirjastavad enne, kui lepingu täitjale võimaldatakse juurdepääs infovarale;

41.2. leping peab sisaldama konfidentsiaalkohustuse nõuete sätteid.

X Infoturbe valdkonda reguleerivad õigusaktid ja standardid

42. Vallas koordineerib infoturbe halduse protsessiga seonduvaid tegevusi IT-juht, võttes arvesse kohustuslikke nõudeid ja üldtunnustatud standardeid ning hea tava soovitusi. Tähtsaimateks õigusaktideks, mis reguleerivad andmekaitset automatiseeritud andmetöötlusel või andmekogude pidamisel, on avaliku teabe seadus, isikuandmete kaitse seadus.

43. Standardid ja hea tava soovitused valitakse ja kasutatakse kooskõlas kehtivate õigusaktidega ning rakendatakse vastavalt organisatsiooni infoturbe vajadustele. Standarditest rakendatakse ISKEt.

44. Infoturbe valdkonna ülataseme dokumendiks on vallavalitsuses infoturbe poliitika. Infoturbe poliitika on strateegiline dokument, mille asjakohasust hindab perioodiliselt IT-juht, kes teeb ettepanekud vajalike muudatuste sisseviimiseks.

45. Vastavalt ülataseme dokumendi tõlgendamise vajadusele võib olemasolevatele dokumentidele lisanduda valdkonda reguleerivaid alampoliitikaid, eeskirju, kordi, tehnilist dokumentatsiooni, standardeid, leppeid, juhendeid vms.

XI Lõppsätted

46. Andmekaitse- ja personalispetsialist tutvustab käesolevat eeskirja uutele teenistujatele enne teenistuja tööle asumist ja ametis olevatele teenistujatele dokumendihaldusprogrammi Amphora kaudu.

47. Käskkiri jõustub teatavakstegemisest.

(allkirjastatud digitaalselt)
Lauri Luur
vallavanem