TÜRI VALLAVALITSUS
KORRALDUS

Türi valla infoturvapoliitika 1. aprill 2026 nr 110

Üldkorraldus on antud kohaliku omavalitsuse korralduse seaduse § 30 lõike 1 punkti 2, Türi Vallavolikogu 30. novembri 2017 määruse nr 10 „Türi valla põhimäärus“ § 60 lõike 1 ja lõike 2 punkti 3 ning Türi Vallavolikogu 26. märtsi 2026 otsuse nr 21 „Türi vallas küberturvalisuse nõuete täitmiseks juhtkonna ülesannete ja pädevuse määramine“ punkti 1.1 alapunkti 2 alusel, arvestades küberturvalisuse seaduse § 3 lõike 2 punkti 4 ja §-s 7 sätestatud teenuseosutaja süsteemi turvameetmeid ning ettevõtlus- ja infotehnoloogiaministri 16. detsembri 2022 määruse nr 101 „Eesti infoturbestandard“ lisa 1 „Nõuded infoturbe halduse süsteemile“ punkte 6.1 ja 6.6.

1. Üldsätted

1.1 Türi valla (edaspidi *valla*) infoturvapoliitika määratleb peamised infoturbe korralduse põhimõtted valla omavalitsusorganite ehk Türi Vallavolikogu (edaspidi *vallavolikogu)* ja Türi Vallavalitsuse kui täitevorgani (edaspidi *vallavalitsus*) ning Türi Vallavalitsuse kui ametiasutuse (edaspidi *ametiasutus*) ja Türi Vallavalitsuse hallatavate asutuste (edaspidi *hallatav asutus*) (ametiasutus ja hallatavad asutused koos on nimetatud edaspidi *valla asutus*) tegevuses.

1.2 Infoturvapoliitikat tuleb arvestada valla õigusaktide eelnõude väljatöötamisel, nähes õigusaktides vajadusel ette ka valla infotruvapoliitika rakendamisega seotud tegevused.

1.3 Valla infoturvapoliitikat on kohustatud järgima vallavolikogu ja vallavalitsuse liikmed, ametiasutuse ametnikud ja töötajad ning hallatavate asutuste töötajad (edaspidi nimetatud ametnik ja töötaja koos *töötaja*), samuti kõik isikud, kes vallaga sõlmitud lepingu alusel või tulenevalt ametiseisundist kasutavad valla infotehnoloogia vara (edaspidi *IT-vara*).

2. Mõisted

2.1 Infoturvapoliitika on koostatud küberturvalisuse seaduse ning selle alusel kehtestatud Eesti infoturbestandardi (edaspidi *E-ITS*) rakendamiseks ning selles kasutatakse mõisteid eelmärgitud õigusaktide ja Riigi Infosüsteemide Ameti veebilehel avaldatud juhendite ja selgituste tähenduses.

2.2 Valla kontekstis on punktis 2.1 viitatud allikatest tulenevate mõistete sisu täpsustatult järgmine:
1) IT-vara on valla ja valla asutuse jaoks väärtust loov tarkvara ja riistvara komponent;
2) kaitseala on kirjeldus, millega piiritletakse valla ja valla asutuse infoturbe ulatus;
3) infoturbe intsident on reaalse või potentsiaalse kahju juhtum, mis võib ohustada IT-vara turvalisust, põhjustades selle tervikluse, käideldavuse või konfidentsiaalsuse kao, sealhulgas toimingud, mis ei ole infoturvet reguleerivate õigusaktidega kooskõlas.

3. Infoturvapoliitika eesmärk, tähtsus ja juhtkonna kohustumus

3.1 Valla infoturbe eesmärk on tagada valla ja valla asutuse toimimise seisukohast oluliste teenuste toimepidevus, protsesside digitaalne kaitse ning valmisolek kriisiolukorras käitumiseks.

3.2 Valla infoturbe tähtsus tuleneb järgmistest asjaoludest:
1) vald ja valla asutus töötleb ulatuslikult isikuandmeid ning nende lekkimine või väärkasutus kahjustaks avalikku usaldust ja rikuks isikuandmete kaitset reguleerivatest õigusaktidest tulenevaid kohustusi;
2) valla põhiteenused sõltuvad järjest enam infosüsteemidest ja infoturbe intsidendid mõjutavad otseselt isikutele teenuste osutamist;
3) kohustusest täita küberturvalisuse seadust, E-ITSi nõudeid, Euroopa Liidu isikuandmete kaitse üldmäärust, isikuandmete kaitse seadust, avaliku teabe seadust ning muid õigusaktidega isikuandmete kaitset ning küberturvalisust nõudvaid kohustusi;
4) valla infosüsteemide ühendatus riiklike andmekogudega eeldab, et vald ja valla asutus täidab oma osa üleriigilise küberturbe tagamisel.

3.3 Vald ja valla asutus rakendab turvaeesmärkide täitmiseks E-ITSi ulatuses, mis tagab ohtude realiseerumisel valla ja valla asutuse ülesannete täitmise jätkumise.

3.4 Valla infoturbe strateegia põhielemendid on:
1) kaitseala- ja riskipõhine lähenemine;
2) konfidentsiaalsuse, tervikluse ja käideldavuse tagamine kõigis kriitilistes teenusprotsessides;
3) proportsionaalsus;
4) pidev parendamine.

3.5 Rakendatavad turvameetmed peavad olema majanduslikult õigustatud ja proportsioonis võimaliku kahjuga, mis võib tekkida meetmete puudulikkuse tõttu, ning nende häiriv toime valla asutuste tegevusele ja töötajate tööle peab olema võimalikult väike.

3.6 Kõiki valla toimimise seisukohalt olulisi muudatusi tuleb enne nende rakendamist kaaluda infoturbe seisukohast. Muutunud nõuete kehtestamise või uute ohtude ilmnemise või intsidentide toimumise korral tuleb turvameetmed ümber hinnata.

3.7 Valla juhtkond (vallavolikogu, vallavalitsus, vallavanem ja valla asutuse juht) kinnitab oma kohustumust infoturbe tagamisel. Juhtkond mõistab, et teabe kaitsmine on osa heast valitsemistavast ning avaliku teenistuse ja avalike teenuste osutamise usaldusväärsuse aluseks. Juhtkond vastavalt oma pädevusele kohustub:
1) tagama infoturbe rakendamiseks piisavad ressursid (eelarvelised, organisatsioonilised, inimressurss);
2) integreerima infoturbe juhtimise valla juhtimis- ja sisekontrollisüsteemi;
3) edendama infoturbekultuuri kogu organisatsioonis;
4) järgima kehtivaid õigusakte ning E-ITSi nõudeid;
5) käsitlema infoturvet pideva protsessina, mitte ühekordse tegevusena.

4. Infoturbe organisatsioon ja vastutusalad

4.1 Valla juhtkonna ülesanded, pädevus ja vastutus küberturvalisuse nõuete täitmiseks on määratud vallavolikogu otsusega.

4.2 Vallavolikogu
1) tagab valla infoturbepoliitika ja infoturbe eesmärkide elluviimiseks ning küberturvalisuse tagamiseks vallaeelarvega vajalikud finantsvahendid ning vastavalt vallavolikogu pädevusele valla asutuse tegevuse korralduse ning vajaliku vara;
2) teeb vallavolikogu pädevusest lähtuvalt valla infoturbe nõuete täitmise üle järelevalvet.

4.3 Vallavalitsus
1) on valla infoturbe eestvedaja ning kinnitab valla infoturbe eesmärgid ja põhimõtted;
2) tagab vallaeelarve eelnõu koostamise ja vallaeelarve täitmisega infoturbe rakendamiseks

vajalikud ressursid (sh eelarvelised ja organisatsioonilised);
3) võtab teadmiseks infoturbe aruanded ja infoturbe meetmete rakendusplaani;
4) otsustab infoturbe riskide aktsepteerimise, infoturbe prioriteedid ja infoturbe tagamiseks olulised parendusmeetmed;
5) tagab, et infoturbe juhtimine on osa valla juhtimis- ja sisekontrollisüsteemist.

4.4 Infoturbealane kaitse valla asutuses tagatakse valla asutuse juhi või asutuse juhtkonna tasemel asutuse tegevusprotsesside ja IT-varade kaardistamise, dokumenteerimise ja ajakohasena hoidmisega ning asutuse infoturbemeetmete rakendamiseks vajalike rahaliste ja mitterahaliste ressursside (sh koolituste korraldamiseks vajalike ressursside) kavandamise ning asutuse töötaja põhitööga kaasnevate infoturbekohustuste aktsepteerimisega.

4.5 Ametiasutus korraldab vallaülese infoturbe halduse ja tagab infoturbe protsesside toimimise. Ametiasutuse ülesanded infoturbe halduses on:
1) tagada valla infoturbe halduse süsteemi rakendamine ja toimimine;
2) töötada välja infoturbe halduse aluspõhimõtted ja koordineerida nende rakendamist;
3) korraldada nõuetest tulenevate infoturbe auditite tellimine;
4) koondada ja esitada vallavalitsusele infoturbe aruanded.

4.6 Valla asutuse juht vastutab asutuse infoturbe halduse süsteemi rakendamise ja infoturbealase kaitse toimimise eest. Asutuse juhi ülesanded on:
1) tagada asutuses infoturbe ja riskijuhtimise põhimõtete rakendamine;
2) tagada asutuses infoturvet reguleerivate juhiste ja dokumentide täitmine ning ajakohasus;
3) osaleda asutuse infoturbe riskide hindamisel ja infoturvameetmete rakendamisel;
4) tagada, et asutuse töötajad on teadlikud infoturbe nõuetest;
5) teavitada asutuses infoturbe eest vastutavat isikut või valla infoturbejuhti olulistest infoturbe intsidentidest.

4.7 Vallas infoturbe eest vastutav isik on vallavalitsuse nimetatud infoturbejuht.
Infoturbejuhi ülesanded on:
1) nõustada vallavalitsust, ametiasutust ja valla asutuste juhte infoturbe küsimustes;
2) koordineerida infoturbe ja riskijuhtimise protsessi;
3) koostada infoturbe aruanded ja iga-aastane infoturbe meetmete rakendusplaan;
4) anda juhiseid turvameetmete rakendamiseks;
5) teavitada Riigi Infosüsteemi Ameti turvaintsidentide käsitlemise osakonda (CERT-EE) olulistest turvaintsidentidest.

5. Riskihaldus

5.1 Riskihalduse metoodika põhineb E-ITSil. Riskianalüüs tehakse valla asutuse tegevusvaldkondades, kus rakendatud standardsed turbemeetmed ei ole piisavad või meetmete mitterakendamisest tulenevad jääkriskid vajavad täiendavat hindamist.

5.2 Kui valla asutuse juht leiab, et E-ITSi põhisest riskianalüüsist asutuse infoturbe korraldamiseks ei piisa, koostatakse detailne riskianalüüs, kus käsitletakse eraldi iga infovarale mõjuvat ohtu, hinnatakse ohu realiseerumise tõenäosust, selgitatakse välja suuremad riskid ja võetakse vajaduse korral kasutusele spetsiifilised meetmed nende vähendamiseks.

5.3 Kui mõnda turvameedet ei ole võimalik või otstarbekas rakendada, siis peab leidma alternatiivsed turvameetmed riski vähendamiseks. Kui ka ühtegi alternatiivset turvameedet ei ole võimalik või otstarbekas rakendada, siis aktsepteeritakse meetme rakendamata jätmisega tekkinud jääkriski.

6. Juurdepääsu haldus

Juurdepääs IT-varadele on rollipõhine ja tagatud tugevate autentimismeetoditega.

7. Andmete turvaline edastamine ja säilitamine

Valla asutus tagab andmete edastamisel ja säilitamisel nende kaitse kaasaegsete ja tunnustatud krüptograafiliste meetmete abil, lähtudes riskipõhisest lähenemisest ja kehtivatest standarditest.

8. Konfidentsiaalsuskohustus

8.1 Konfidentsiaalsuskohustus kehtib asutusesiseseks kasutamiseks mõeldud teabele ega sõltu isiku teenistus- või töö tegemise asukohast. Konfidentsiaalsuskohustus kohaldub ka valla asutuse koosseisuvälistele paktikantidele või asutuse tegevusega seotud isikutele, kellel puuduvad otsesed IT-varade kasutamise volitused.

8.2 Kui isik tegutseb valla asutuses lepingu (v.a tööleping) alusel, peab leping sisaldama konfidentsiaalsuskohustuse sätteid.

8.3 Kui IT-varadega seotud lepingulisi kohustusi täidab teine isik, siis peab valla ja teise poole vahel sõlmitud leping sisaldama konfidentsiaalsuskohustuse sätteid. Enne lepingu sõlmimist ei võimalda vald lepingu täitjale juurdepääsu IT-varadele.

9. Infosüsteemide ja muude IT-varade kasutusele võtmine ja muudatused

9.1 Infosüsteemi kasutusele võtmise kavandamisest alates rakendatakse infosüsteemi turvanõuetele vastavaid turvameetmeid.

9.2 Uut infosüsteemi ja selle komponente tuleb enne kasutuselevõtmist või oluliste muudatuste tegemist testida ja tulemused dokumenteerida.

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

10. Infosüsteemide ja muude IT-varadega seotud teenuste või toodete väljast tellimine

Väljastpoolt tellitavate IT-teenuste lepingud peavad tagama nõutava turvataseme ning sisaldama infoturbe- ja konfidentsiaalsussätteid.

11. Infoturbealane teavitus ja koolitus

11.1 Üldist infoturbealast teavet jagatakse valla veebilehel www.tyri.ee, valla siselistide kaudu ja võimalusel valla asutuse siseveebis.

11.2 Infoturbealast teavet saadetakse e-posti teel. Infoturbe intsidentidest teavitatakse viivitamata asutuse IT-osakonda või IT-teenusepakkujat ning valla infoturbejuhti, kes hindab olukorda ja korraldab vajalikud reageerimismeetmed.

11.3 Töötajate infoturbekoolitus hõlmab iseseisvat õpet juhendite põhjal, konsultatsioone ja valla asutuse juhi või ametiasutuse korraldatavaid sisekoolitusi. Täpsemalt määratakse sisekoolitused asutuse iga-aastases koolitusplaanis või muudes valla asutuse dokumentides.

11.4 Valla asutuse töötaja peab kord kahe aasta jooksul tegema kübertesti.

12. Kaugtöö

12.1 Kaugtöö valla asutuses on lubatud kokkuleppel vastava asutuse juhiga.

12.2 Kaugtöö on lubatud tingimusel, et töötaja tagab ülesannete täitmisel sama turvataseme kui teenistus- või töökohal töötades.

13. Tulemuslikkuse hindamine

13.1 Infoturbe tulemuslikkuse hindamine on pidev protsess, mille eesmärk on kontrollida, kas rakendatud turvameetmed tagavad soovitud turvataseme ning kas infoturbe halduse süsteem toimib tõhusalt.

13.2 Tulemuslikkuse hindamise põhimõtted on mõõdetavus, läbipaistvus ning pidev parendamine.

13.3 Tulemuslikkuse hindamise meetodid hõlmavad:
1) sisemist auditit, mis hindab infoturbe halduse süsteemi vastavust E-ITSi nõuetele;
2) küberturvalisuse taseme jälgimist kübertestide ja haavatavusanalüüside kaudu;
3) intsidentidele registreerimist, analüüsi ning tagasiside rakendamist tulevaste riskide maandamiseks;
4) töötajate teadlikkuse ja koolituste tulemuslikkuse hindamist.

13.4 Valla infoturbejuht koostab igal aastal infoturbe olukorra aruande, mis sisaldab hinnangut turvameetmete toimivusele, intsidentide kokkuvõtet, auditi tulemusi ja ettepanekuid parendusmeetmeteks. Aruanne esitatakse vallavalitsusele läbivaatamiseks ja kinnitamiseks.

13.5 Infoturbe tulemuslikkuse hindamise tulemused on aluseks infoturvapoliitika ja seonduvate dokumentide uuendamisel ning järgneva perioodi infoturbe meetmete rakendusplaani koostamisel.

14. Infoturvapoliitikaga seotud dokumendid ja poliitika muutmine

14.1 Valla infoturvet reguleerivad juhendid ja korrad koostatakse lähtuvalt infoturvapoliitikast ja E-ITS standardist ning tehakse kättesaadavaks kõigile, kes peavad neid järgima.

14.2 Valla infoturbe dokumentatsiooni kuulub infoturbekontseptsioon, mis sisaldab täpsemaid eesmärke ja rakendusplaani valitud E-ITS meetmete rakendamise kirjeldust.

14.3 Muud juhised ja hea tava reeglid kehtestatakse kooskõlas kehtivate õigusaktidega ning rakendatakse vastavalt vajadusele.

14.4 Infoturvapoliitikat muudetakse, kui:
1) seda nõuavad turvaauditi tulemused;
2) muudatuse vajadus tuleneb E-ITS uue versiooni ilmumisest;
3) muudatuste vajaduse tingivad olulised tehnilised, organisatsioonilised või õiguslikud muutused või muud sisemised või välised asjaolud.

(allkirjastatud digitaalselt)

Sulo Särkinen
vallavanem

(allkirjastatud digitaalselt)

Lii Laanemets
vallasekretär