



M Ä Ä R U S

Narva

28.04.2021 nr 9

Narva linnavalitsuse infoturbe kord

Määrus kehtestatakse kohaliku omavalitsuse korralduse seaduse § 30 lõike 1 punkti 3 alusel

§ 1. EESMÄRK JA PÕHIMÕTTED

- (1) Infoturbe kord määrab Narva linnavalitsuse ja Narva linna struktuuriüksuste (edaspidi *linnavalitsus*) suunised oma infovarade turvalisuse tagamisel. Linnavalitsus väldib oma infovarade ja oma maine kahjustamist rakendades piisavaid turvameetmeid võimalike ohtude ilmumise tõenäolisemates valdkondades, mis aitab kaasa katkestuseta tegevuse tagamisele linnavalitsuse struktuuriüksustes. Valitud turvameetmed peavad aitama täita õigusaktidest tulenevaid turvanõudeid ning olema majanduslikult õigustatud. Nende toime ei tohi ülemääraselt häirida töötajate tööd.
- (2) Infoturbe kord seab turbe eesmärgid, nende saavutamise suunised, üldise turbe strateegia ja korralduse ning peamiste turvamehhanismide rakendamise viisid.
- (3) Linnavalitsus lähtub infoturbe korraldamisel info- ja kommunikatsioonitehnoloogia (edaspidi IT) halduse headest tavadest ja Eesti infoturbe standardi juhistest. Turvadokumentide koostamisel kasutatakse E-ITS mudeleid ja mõisteid.
- (4) Linnavalitsuse infoturbepoliitika hõlmab kõiki linnavalitsuse struktuuriüksusi ja kehtib kõigis linnavalitsuse struktuuriüksustes. Infoturbe korra elluviimise tagab linnakantselei.

§ 2. MÕISTED

- (1) Infoturbe - teabe ja infosüsteemide loomine nõuetekohaste reeglite järgi ja kaitsmine loata juurdepääsu, kasutamise, avaldamise, muutmise või hävitamise eest.
- (2) Äriprotsess - kogum loogiliselt seotud tegevusi (ülesandeid, töövooge), mis sooritatakse avalike ülesannete täitmisel või organisatsiooniliste eesmärkide saavutamiseks.
- (3) Infovara (sihtobjekt) - informatsioon, andmed ja nende töötlemiseks vajalikud süsteemne tarkvara ja rakendused ning riistvara ja võrgu seadmed. Sihtobjekt võib olla füüsiline, näiteks võrk või IT-süsteem. Sageli on aga sihtobjektideks loogilised objektid, näiteks organisatsiooni allüksused, rakendused või kogu infosüsteem.
- (4) Kaitsetarve - näitab, milline kaitse on äriprotsessile, selles töödeldavale informatsioonile ja rakendatavale infotehnoloogiale piisav ja sobiv.
- (5) Andmekogu on kohaliku omavalitsuse või avalikke ülesandeid täitva eraõigusliku isiku infosüsteemis töödeldavate korrastatud andmete kogum, mis asutatakse ja mida kasutatakse seaduses, selle alusel antud õigusaktis või rahvusvahelises lepingus sätestatud ülesannete täitmiseks.
- (6) Logi - arvuti tegevuse päevik, mida kasutatakse nii statistilistel eesmärkidel kui ka varundamise ja taaste jaoks ning arvutivõrgus toimuva analüüsiks.
- (7) Alusohtude kataloog - sisaldab võimalike infotehnoloogia ohtude kirjeldusi, mis on liigendatud vääramatu jõu, korralduslike puuduste, inimvigade, tehniliste tõrgete ja sihilike toimingute teemade järgi.
- (8) 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.
- (9) Andmete omanik – isik, kes vastutab andmete loomise, klassifitseerimise, kasutamise, ligipääsude reguleerimise ja administreerimise eest terve andmete elutsükli jooksul.

- (10) Krüpteerimine - andmete teisendamine sellisele kujule, mida teistel isikutel on võimalik lugeda ainult vastava dekrüpteerimise võtme abil.
- (11) Infoturbe intsident - mistahes kõrvalekalle süsteemide normaalsest talitlusest ja kasutajate tavapärasest käitumisest.
- (12) Varundamine - andmete koopia loomine, mis on salvestatud algsest asukohast erinevasse asukohta ja võimaldab taastada algsed andmed.
- (13) Andmete hävitamine - andmekandjal olevate andmete töötlemine viisil, et andmekandjalt või selle jäänustelt/tükkidelt ei oleks sinna salvestatud andmed enam loetavad.

§ 3. VASTUTUS

- (1) Kõik linnavalitsuse teenistujad ja töötajad vastutavad oma töövaldkonnas turbeesmärkide saavutamise ja kehtestatud kordade täitmise eest.
- (2) Üldvastutus infoturbe tagamise eest on linnapeal ja linnasekretäril vastavalt pädevusele.
- (3) Infoturbealast tööd koordineerib linnasekretäri poolt kokku kutsustud IT nõukogu kaasates infoturbe töögrupp. Infoturbe eesmärkide elluviimist korraldab infoturbe juht koos IT juhiga.
- (4) Iga struktuuriüksuse infoturbe eest vastutab selle üksuse juhataja.
- (5) Konkreetsete turvameetmete rakendamise eest vastutaja määratakse linnasekretäri ja/või linnapea käskkirjaga või on määratud töötaja ametijuhendites.
- (6) Vastutavate töötajate eemaloleku ajaks tuleb neile määrata ajutised asetäitjad.
- (7) Väline audit tellitakse vastavalt vajadusele, aga mitte harvemini kui kord kolme aasta jooksul.

§ 4. ÄRIPROTSESS

- (1) Infoturbe ülesanne organisatsioonis on säilitada äriprotsesside käigus töödeldava teabe turvalisus.
- (2) Infoturbe konkreetsed eesmärgid – kaitseala, kaitsetarve, sihtobjektid ja turbeviis määratakse lähtuvalt äriprotsessidest, mis on vastavuses linnavalitsuse tegevuse eesmärkidega.
- (3) Igale äriprotsessile määratakse omanik.
- (4) Äriprotsessi omanik koostab äriprotsessi riskianalüüsi.

§5. INFOVARAD

- (1) Narva linnavalitsuse struktuuriüksuste tööks soetatud infovarade, sh töötajate poolt loodud infovarade, omanik on Narva linn.
- (2) Infovarade üle peavad arvestust IT teenistus, rahandusameti raamatupidamise osakond ja ametid vastavalt oma töövaldkonnale. Iga vastutav teenistus kehtestab asjakohased protseduurid. Kõik struktuuriüksused edastavad andmed infovara kohta linnakantselei IT teenistusele.
- (3) Linnavalitsuse andmekogude kaitsetarve (turbeklassid) kinnitatakse andmekogude põhimäärustes.
- (4) Lähtuvalt linnavalitsuse infovarade kaitsetarbest hinnatakse linnavalitsuse infovaradele asjakohaste turvameetmete rakendamise vajadust ja koostatakse meetmete rakendusplaani.
- (5) Linnavalitsuse infovarade ja neile rakenduvate turvameetmete rakendatus vaadatakse läbi vähemalt kord aastas linna eelarve koostamisega koos või suuremate muutuste ja kriitiliste intsidentide korral. Läbivaatust koordineerib infoturbe juht. Läbivaatusel analüüsib infoturbe juht koos töös IT juhi ja äriprotsesside (andmete) omanikega ja struktuuriüksuste vastutavate spetsialistidega.
- (6) Üldjuhul võib töötaja teha oma tööülesannete täitmiseks linnavalitsuse andmetest koopiaid. Keelatud on teha koopiaid konfidentsiaalsetest andmetest ja riiklike andmekogude andmetest ning viia neid välja töökohalt või/ja anda neid teistele isikutele, välja arvatud seadustest tulenevad juhud.

§ 6. ÜLDTURVE

- (1) Üldturvet korraldab linnasekretär koos IT nõukogu, infoturbe juhi ja struktuuriüksuste juhtidega.
- (2) Üldturve reguleeritakse töökorra reeglistiku, arvutivõrgu kasutamise eeskirja ja teiste õigusaktidega.
- (3) Kõigi uste võtmete arvu ja jagamise üle tuleb pidada kirjalikku arvestust.
- (4) Ligipääs olulistele ruumidele tagatakse tööalase vajaduse ja vastuse alusel. Olulistes ruumides peab olema paigaldatud valvesignalisatsioon ning tagatud reageerimisvõimekus häirele.
- (5) Tööruumis tuleb viimasel väljujal sulgeda aknad ja lukustada uks.
- (6) Väline hoolde- ja remondipersonal lubatakse ruumidesse ainult koos saatjaga.

§ 7. PERSONALI TURVE

- (1) Personali töөлövõtul tuleb uuele töötajale tutvustada infoturvet reguleerivaid eeskirju.
- (2) Ametijuhendisse või töölepingusse tuleb lisada asjakohased turva- ja konfidentsiaalsusnõuded.
- (3) Töösuhte lõppemisel peab töötaja tagastama kõik tema valduses olevad linna varad ja pääsuvahendid ning kõik pääsuõigused tühistatakse viimase tööpäeva lõpuks.
- (4) Töötajaid tuleb teavitada neid puudutavate infoturbe meetmete muutustest ja uutest turvaohutusest viivitamatult.
- (5) Töötajale peab olema tagatud infoturbealane koolitus.

§ 8. JUHISDOKUMENDID

Linnavalitsuse infoturbe üldised korrad kehtestab linnavalitsus. Täpsemad infovarade ja nende turvameetmete loetelu, krüpteerimise korra, infosüsteemi kasutajate ja teenindajate õigused ning kohustused infosüsteemi töökindluse ja kasutusmugavuse tagamisel, infosüsteemi varundamise ning muud infoturvet reguleerivad korrad kehtestab linnakantsleil.

§ 9. ANDMETE JA DOKUMENTIDE TURVE

- (1) Linna õigusaktidega määratakse igale infovarale omanik, kes võib volitada teisi töötajaid olema vastutav andmete töötlemisel.
- (2) Andmete omanik või vastutav isik korraldab andmete tehnilise haldamise ja administreerimise andmete omaniku eest ja vastavalt andmete omaniku poolt esitatud nõuetele infotehnoloogiliste ja muude vahenditega.
- (3) Andmete omanik koos infoturbe juhiga viib läbi oma vastutusala infovarade riskianalüüsi.
- (4) Kõiki tööalaseid andmeid hoitakse struktuuriüksuse, teenistuse või igale töötajale eraldatud võrgukettal. Tööalaste andmete hoidmine töötaja arvutis ei ole soovitatav, sest neid andmeid ei varundata ning töötaja arvutis olevate andmete säilimise eest vastutab töötaja.
- (5) Sülearvutite kataloogi My Documents sisu sünkroniseeritakse võrgukettaga kord ööpäevas.
- (6) Struktuuriüksuste vaheline dokumentide ja andmekandjate saatmine/ üleandmine ning vastuvõtmine tuleb kirjeldada dokumendiregistris kirja sisestaja poolt vastavalt dokumendiregistri kasutamise juhistele.

§ 10. PÄÄSUPOLIITIKA

- (1) Juurdepääs infovaradele peab olema korraldatud tööalase vajaduse ja vastutuse alusel.
- (2) Pääsuparoolide tuleb vahetada vastavalt arvutivõrgu kasutamise eeskirjale või andmekogu põhimääruses sätestatud korras ja tähtaegade.
- (3) Süsteemiparoolid peavad olema deponeeritud turvalises asukohas krüpteeritud ning varustatud kasutusjuhustega. Isikute ringi, kellel on neile juurdepääs, määrab linnasekretär.
- (4) Oluliste ruumide varuvõtmed deponeeritakse pitseerituna turvalises asukohas linnasekretäri poolt määratud isiku juures.

§ 11. INFOVAHETUSE TURVE

- (1) Väljapool tööruume töödeldavatel andmekandjatel olevad konfidentsiaalsed andmed peavad olema krüpteeritud.
- (2) Süsteemiligid tuleb säilitada vähemalt neli nädalat ja nende ülevaatus tuleb sooritada vähemalt kord kuus või vastavate turvaintsidentide korral.
- (3) Tagada tuleb kõigi tarbetute konfidentsiaalsete andmetega paberdokumentide ja andmekandjate hävitamine.
- (4) Töökohtade arvutitest, mis sisaldavad konfidentsiaalseid andmeid, tuleb remonti saatmisel või utiliseerimisel neis sisalduvad andmed eelnevalt hävitada.
- (5) Töökohtades ja e-posti süsteemis peab olema rakendatud keskne viirustõrje.
- (6) Linnavalituse sisevõrku ühenduvad arvutid alluvad kesksele juhtimisele ja administreerimisele.
- (7) Kesksest kontrollitakse ja logitakse töökoha arvutitesse sisenemist ja nende kasutamist. Kesksest hallatakse arvuti kasutamise võimalusi kasutajagruppide lõikes ning kontrollitakse turvalist arvutikasutust.

§ 12. VARUNDAMINE

- (1) Andmete varundamine korraldatakse vastavalt Andmevarundamise ja arhiveerimise korrale.
- (2) Vastutav isik vastutab keskse süsteemi varukoopia tegemise eest. Vähemal 1 kord aastas tuleb luua vajalikest andmetest varukoopia püsisäilituseks.
- (3) Kasutajal on võimalik avada linnavalitsuse serveril tööalaseks otstarbeks andmete salvestusmaht.

§ 13. INFOTURBE INTSIDENTIDE KÄSITLEMINE

- (1) Infoturbe intsidentide käsitlemise eesmärk on tagada turvaintsidentidest tuleneva kahju minimeerimine.
- (2) Üksikasjalikud juhised on Infoturbe intsidentide käsitlemise korras.
- (3) Infoturbe intsidentidest ja vastumeetmete rakendamise mittevastavustest tuleb teavitada viivitamatult IT juhti ja infoturbe juhti.
- (4) Infoturbe eest vastutav isik peab tagama intsidendile reageerimise, registreerimise ja hilisema analüüsi.
- (5) Intsidentide analüüsi kasutatakse alusmaterjalina turvameetmete rakendamise plaani koostamisel ja uuendamisel.

§ 14. INFOTURBE KORRA ÜLEVAATUS JA MUUTMINE

- (1) Infoturbe korra ülevaatus peab tagama infoturbe nõutava taseme säilimise.
- (2) Seadusandluse või turbeolukorra muutumisel tuleb linnapeal ja/või linnasekretäril ning infoturbe juhil algatada infoturbe alusdokumentide ja meetmete muutmise protsess.
- (3) Infoturbe korra ülevaatus toimub kord aastas või peale suuremaid muutusi organisatsioonis, süsteemides või regulatsioonides või pärast kriitilist intsidenti.
- (4) Läbivaatuse ja värskendamise korraldab infoturbe juht koos IT nõukoguga.
- (5) Muudatustest teavitatakse kõiki töötajaid, keda see puudutab.
- (6) Linnavalitsus vaatab kord aastas üle infoturbe olukorra ja talitluspidevust tagavate meetmete kava.
- (7) IT nõukogu vaatab infoturbe olukorra aruande läbi kord kvartalis.

§ 15. JÄRELEVALVE

- (1) Järelevalvet infoturbe poliitika täitmise üle korraldab infoturbe juht.
- (2) Infosüsteemide vastavust infoturbe korrale kontrollitakse sise- ja välisaudititega.

§ 16. RAKENDUSSÄTTED

1. Tunnistada kehtetuks Narva Linnavalitsuse 21.augusti 2013.a määrusega nr 32 kinnitatud "Narva Linnavalitsuse infoturbe kord"
2. Määrus jõustub seadusega sätestatud korras.



Katri Raik
Linnapea



Üllar Kaljuste
Linnasekretär