LOKSA LINNAPEA

K Ä S K K I R I

Loksa linn 06. september 2023 nr 3

Loksa Linnavalitsuse infoturvapoliitika

Käskkirja vastuvõtmise aluseks on kohaliku omavalitsuse korralduse seaduse § 50 lõike 1 punkt 3 ja küberturvalisuse seaduse § 7 lõike 1 punktid 1 ja 2 ning Riigi Infosüsteemi Ameti juhendid.

I INFOTURBE RAKENDUSALA JA ORGANISATSIOON

1. Infoturbe rakendusala ja infoturvaeesmärgid

1.1. Infoturvapoliitika dokument on eeskirjade kogum, mis reguleerib infovarade haldust ja kaitset Loksa Linnavalitsuses (edaspidi *asutus*).
1.2. Infoturvapoliitika eesmärk on määratleda peamised infoturbe valdkonnad infoturbe eesmärgi saavutamiseks.
1.3. Infoturvaeesmärkideks on tagada asutuse põhitegevuse toimimine ja tööprotsesside infovarade terviklus, käideldavus ja konfidentsiaalsus.
1.4. Info terviklus, käideldavus ja konfidentsiaalsus tuleb tagada ulatuses, mis võimaldab asutusel kõige tõenäolisemate ohtude realiseerumisel häireteta oma ülesandeid täita.
1.5. Turvameetmed peavad olema majanduslikult õigustatud ja proportsioonis võimaliku kahjuga, mis võib tekkida meetmete puudulikkuse tõttu ning nende häiriv toime asutuse tegevusele ja teenistujate tööle peab olema võimalikult väike.

2. Ülevaade organisatsioonist

2.1. Asutuse põhitegevus on sätestatud kohaliku omavalitsuse korralduse seaduse paragrahvis 6.
2.2. Asutus töötleb oma põhitegevusest lähtuvalt infot, millega kaasneb mh isikuandmete töötlemine ning muude andmete töötlemine, mille saladuses hoidmiseks on kolmandal osalisel õigustatud huvi.
2.3. Infoturvapoliitikat on kohustatud oma teenistusülesannete täitmisel järgima kõik asutuses töötavad ametnikud ja töötajad (edaspidi *teenistujad*).

3. Info tundlikkuse tasemed

3.1. Asutuses kasutatav info jaguneb järgmiselt:
3.1.1. konfidentsiaalne,
3.1.2. mittekonfidentsiaalne.
3.2. Konfidentsiaalne info sisaldab:
3.2.1. isikuandmeid ja andmeid, mille saladuses hoidmiseks on kolmandal osalisel õigustatud huvi.

4. Asutuse sõltuvus infotehnoloogia kasutamisest

4.1. Asutuse põhiprotsesside toimimine on ilma infotehnoloogiata oluliselt raskendatud.
4.2. Asutuse enamiku teenistujate peamine töövahend on arvuti.

5. Standardid

5.1. Asutus lähtub infoturbe tegevustes Eesti infoturbestandardi (E-ITS) metoodikast ning E-ITS meetmete kataloogist ja juhenditest.

II INFOTURBE ORGANISATSIOON JA VASTUTUS

6. Juhtkond
6.1. Üldvastutus infoturbe tagamise eest on asutuse juhil ehk linnapeal.
6.2. Infoturbe jääkriskid hindab ja aktsepteerib linnapea.

7. Infoturbe töörühm
7.1. Infoturbe töörühma määrab linnapea käskkirjaga.
7.2. Infoturbe töörühma kohustused on järgmised:
7.2.1. infoturbe järjepidev kavandamine ja korraldamine;
7.2.2. infoturbe dokumentide koostamine ja menetlemine;
7.2.3. infoturbe järelevalve;
7.2.4. infoturbeteadlikkuse tõstmise korraldamine;
7.2.5. infoturbeintsidentide menetlemine;
7.2.6. linnapeale perioodiliste ja sündmuste põhiste aruannete esitamine,
7.2.7. erandite kooskõlastamine.

8. Juhtivametnikud
8.1. Juhtivametnike (abilinnapead, linnasekretär, pearaamatupidaja) kohustused on järgmised:
8.1.1. infovarade käideldavuse, tervikluse ja konfidentsiaalsuse ning infovarade kaitset korraldavate õigusaktide täitmise tagamine oma valdkonna teenistujate poolt;
8.1.2. kõigi vahetute alluvate teavitamine kehtivatest infoturbega seotud haldusaktidest;
8.1.3. kõigi vahetute alluvate infosüsteemi kasutamise õiguspärasuse ja infosüsteemi toimimise õiguspärasuse jälgimine;
8.1.4. infoturbe probleemidest teatamine, asjakohaste ettepanekute tegemine ja tagasiside andmine turbealaste haldusaktide toimimise kohta.

9. Teenistujad
9.1. Kõik teenistujad vastutavad:
9.1.1. oma töövaldkonnas infoturbe eesmärkide saavutamise ja kehtestatud kordade täitmise eest;
9.1.2. kõigi tema kasutusse antud infosüsteemi komponentide säilimise ning turbe eest.

III TURVALISUS

10. Riistvara ja tarkvara turve
10.1. Riist- ja tarkvara ning nende andmete tervikluse, käideldavuse ja konfidentsiaalsuse kaitseks tuleb korraldada:
10.1.1. rakendustele ja andmetele juurdepääs;
10.1.2. serverite, töökohaarvutite ja mobiilseadmete turve;
10.1.3. isikuandmete töötlemiseks kord ja kasutatavate seadmete dokumenteerimine;
10.1.5. riist- ja tarkvara muudatuste (konfiguratsiooni) haldus;
10.1.6. IT-vahendite hooldus ja remont;
10.1.7. kolimine,
10.1.8. kaugtöö.

11. Side ja infovahetuse turve
11.1. Infotöötlusvahendite õigeks ja turvalise käitluseks ning kaitseks tuleb korraldada:
11.1.1. võrgutaristu haldus;
11.1.2. tulemüüri haldus;
11.1.3. internetiühenduse haldus;

11.1.4. wifi-haldus;
11.1.5. paberdokumentide ja elektrooniliste andmekandjate turve;
11.1.6. info edastamise turve nii suuliselt kui e-kirja, telefoni jm sidevahendite kaudu.

12. Füüsiline turve
12.1. Lubamatu füüsilise juurdepääsu vältimiseks asutuse teabele, nende kahjustamisele või häirimisele tuleb korraldada:
12.1.1. sissepääs hoonesse ja ruumidesse;
12.1.2. pääsulubade (võtmete, koodide) haldus;
12.1.3. valvesüsteemide paigaldus ja haldus;
12.1.4. tuleohutuse tagamine;
12.1.5. eriruumide paiknemine ja sissepääs;
12.1.6. seadmete paigutus ja kaitse;
12.1.7. töökohtade turve.

13. Personali turve
13.1. Teenistujatest põhjustatud varguse, pettuse või varade väärkasutuse riski vähendamiseks tuleb korraldada:
13.1.1. tööle võtmise tingimused;
13.1.2. turvateadlikkus ja -koolitus;
13.1.3. töösuhte lõpetamine või muutmine.

14. Jätkusuutlikkus
14.1. Põhitegevuse katkestuste vältimiseks ning põhiprotsesside kaitsmiseks infosüsteemide tõrgete või avariide eest ning nende protsesside õigeaegse tagamise jätkamiseks tuleb korraldada:
14.1.1. varundamine ja taastamine;
14.1.2. kontrolljälgede loomine, haldus ja analüüsimine.

15. IKT-teenuste väljast tellimine
15.1. Tagamaks, et infotehnoloogiaga seonduvate teenuste väljast tellimine ei halvendaks asutuse infoturbe olukorda, tuleb korraldada:
15.1.1. teenusepakkuja valimine;
15.1.2. tingimused ja kokkulepped,
15.1.3. lepingu lõpetamine.

16. Varundamine
16.1. Standardtarkvaral põhinevate andmebaaside andmete varundamise intervall ning varukoopiate säilitamise aeg lepitakse kokku standardlahenduse pakkujaga teenuse osutamise lepingus või sätestatakse kohaliku andmekogu põhimääruses.
16.2 Töökohaarvutitesse salvestatud failid sünkroniseeritakse jooksvalt OneDrive-i.

17. Infoturbe kontseptsioon
17.1. Infoturbe kontseptsiooni dokumentatsioon koosneb E-ITS rakendamisel koostatud regulatsioonidest.
17.2. Infoturbe kontseptsiooni dokumentatsioon sisaldab juurdepääsupiirangutega andmeid ja sellele antakse juurdepääs vaid õigustatud teadmisvajaduse alusel.
17.3. Infoturbe kontseptsiooni dokumentatsioon
• Infoturvapoliitika
• Arvutivõrgu, infosüsteemide ja mobiilsete seadmete kasutamise ning infoturbeintsidentide käsitlemise kord
• Infosüsteemide koondtabel
• Võrguskeem koos tööjaamade kirjeldusega
17.4. Punktis 17.3 väljatoodud infoturbe kontseptsiooni dokumentatsiooni kuuluvate dokumentide loetelu ei ole täielik. Loetelu täiendatakse vajadusel E-ITSi rakendamise käigus.

18. Turvanõuded

18.1. Infovara peab olema tuvastatud ning selle turbevajadus peab olema määratletud turvaanalüüsiga. Infovarale rakendatakse otstarbekohaseid infoturbemeetmeid.
18.2. Infovarale peab olema määratud personaalne vastutaja.
18.3. Infovara peab olema kaitstud volitamata juurdepääsu eest ja juurdepääs infovarale antakse vastavalt tööülesannetest tulenevale teadmisvajadusele.
18.4. Infovara kasutajad ja nende poolt teostatavad toimingud peavad olema üheselt tuvastatavad.
18.5 Infovara kasutamist ning turvet reguleerivate eeskirjade tundmine ja järgimine on kohustuslik kõikidele infovara kasutajatele.
18.6. Tööalane info on mõeldud ainult tööalaseks kasutamiseks ja seda ei tohi väljastada ilma õigusliku aluseta ega edastada isiklikule e-posti aadressile.
18.7. Infovara ühiskasutamisel teiste isikutega tuleb tagada teabe õiguspärane töötlemine ja kaitse.
18.8. Kriitilise infovara kohta peab eksisteerima taasteplaan, mis kirjeldab protseduurid kuidas naasta tegevuse juurde, mille katkestas intsident. Plaani peab hoidma ajakohasena ja toimimist kord aastas koostöös teenusepakkujaga testima. Kriitiliste infovarade loendit haldab infoturbejuht.
18.9. Turvaintsidendi korral võib infovara kaitseks piirata selle kasutamist infosüsteemi omaniku või infoturbejuhi ettepanekul.
18.10. Andmete turvaliseks töötlemiseks tuleb kindlustada nõuetele vastav keskkond ja infoturbe kohustuste täitmine, sh andmete käideldavus, terviklus ja konfidentsiaalsus õigusaktis sätestatud kujul.
18.11. Andmed peavad olema otstarbekohased, andmete vajaduseta kopeerimine või koopiate arvu suurendamine ei ole lubatud. Mittevajalikud andmed tuleb selleks volitatud isiku poolt õigeaegselt hävitada.
18.12. Teenistuja peab teenistussuhte ajal ja pärast teenistusest vabastamist hoidma konfidentsiaalsena talle teenistuse tõttu teatavaks saanud tööalast teavet.
18.13. Andmete töötlemiseks võib kasutada ainult infoturbejuhi poolt aktsepteeritavaid infotöötlusvahendeid (näiteks riistvara, tarkvara, andmekandjad, arvutivõrk, heaks kiidetud pilveteenused jne).
18.14. Juurdepääsupiiranguga andmete kasutamine testimise või koolitamise eesmärgil on vaikimisi keelatud. Erandite tegemine peab olema möödapääsmatu ja kirjalikult taas esitaval kujul põhjendatud. Erandi kehtestamise pädevus on infoturbejuhil.
18.15. Turvameetmed peavad enne infosüsteemi või selle muudatuse kasutusele võtmist toimima plaanipäraselt. Ebapiisava turvalisusega infosüsteeme või nende muudatusi on keelatud paigaldada töökeskkondadesse.
18.16. Turvateadlikkuse kindlustamiseks tuleb viia läbi infoturbekoolitusi ja täiendusteavitusi. Teenistujatel on kohustus sooritada positiivselt kord aastas infoturbe test.
18.17. Turvameetmetes erandit lubamise pädevus on infoturbejuhil.

IV RAKENDUSSÄTTED

19. Rakendussätted

19.1. Loksa linnapea 30.12.2019 käskkiri nr 1 „Loksa Linnavalitsuse infoturbepoliitika kinnitamine“ tunnistatakse kehtetuks.
19.2. Juhiabil teha käesolev infoturbepoliitika allkirja vastu teatavaks Loksa Linnavalitsuse teenistujatele.
19.3. Käskkiri jõustub 06. septembril 2023.

/allkirjastatud digitaalselt/

Värner Lootsmann
linnapea