LOKSA LINNAPEA

K Ä S K K I R I

Loksa linn 06. september 2023 nr 4

Loksa Linnavalitsuse arvutivõrgu, infosüsteemide ja mobiilsete seadmete kasutamise ning infoturbeintsidentide käsitlemise kord

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 ARVUTIVÕRGU KASUTAMISE KORD

1. Üldsätted

1.1. Käesoleva korraga sätestatakse Loksa Linnavalitsuse (edaspidi *linnavalitsus*) arvutivõrgu kasutamise nõuded, sh kasutusõiguse andmine ja haldamine, kasutajate ning IT-spetsialisti õigused ja kohustused, ligipääsuõigused ning postiloendi ja elektronposti pseudonüümi haldamine.
1.2. Käesolev kord kehtib kõikidele linnavalitsuse arvutivõrgu teenuste ja ressursside kasutajatele ja kõikide arvutivõrku ühendatud seadmete ja tööjaamade (arvuti, sülearvuti, mobiilne seade jne) kohta ning seda on kohustatud täitma kõik linnavalitsuse teenistujad, linnavalitsuse liikmed, volikogu liikmed ja töövõtu- või muu lepingu alusel teenust osutavad isikud, kes kasutavad linnavalitsuse arvutivõrku (edaspidi *teenistujad*).
1.3. Linnavalitsuse arvutivõrk koosneb ühiseid ressursse ja teenuseid kasutavatest infotehnoloogilistest vahenditest (riist- ja tarkvara) ning nende abil töödeldavatest andmetest.
1.4. Arvutivõrgu kasutajakonto annab kasutajale õiguse kasutada tema tööjaama (arvutit), linnavalitsuse arvutivõrku, infosüsteeme, internetti jms.
1.5. Käesolevas korras nimetatud teavitused ja taotlused jms tuleb esitada vähemalt kaks tööpäeva ette elektrooniliselt IT-spetsialistile, lisades koopiasse linnasekretäri.

2. Arvutivõrgu kasutajakonto loomine

2.1. Kasutajakonto loob IT-spetsialist.
2.2. Kasutajakonto loomiseks ja aktiveerimiseks saadab linnavalitsuse personalitöötaja IT-spetsialistile teavituse, mis sisaldab uue kasutaja ees- ja perekonnanime, isikukoodi, ametikohta, tööle asumise kuupäeva ja lõppkuupäeva, kui see on teada.
2.3. Kasutajatunnus on elektronposti kujul eesnimi.perekonnanimi@loksa. Nimes esinevad tähed õ, ä, ö, ü, š, ž asendatakse tähtedega o, a, o, u, s, z.
2.5. Kasutajanimi ja esmane parool antakse uuele kasutajale IT-spetsialisti poolt isiklikult üle, misjärel kasutaja muudab parooli esimesel sisselogimisel ära.
2.6. Arvutivõrgu kasutusõigus on personaalne ja seda ei ole lubatud teisele isikule edasi anda.
2.7. Isikule, kellele peab kasutusõiguse/ligipääsu võimaldama seaduse alusel, antakse vastav õigus õigusaktis tulenevate ülesannete täitmiseks ja õigusaktis ettenähtud ajaks.
2.8. Personalitöötaja teavitab IT-spetsialisti kasutaja andmete muutumisest (nt nimemuutus). IT-spetsialist teeb kasutaja andmetes ja juurdepääsuõigustes vastavad muudatused.

3. Teenistussuhte peatumine

3.1 Teenistussuhte peatumisel kauemaks kui 90 päevaks teavitab personalitöötaja IT-spetsialisti teenistuja teenistussuhte peatumisest ning lisab täpse kuupäeva.
3.2 Teenistuja on kohustatud enne teenistussuhte peatumist kustutama oma võrguketastelt, pilvest ja elektronpostist isiklikud (teenistusülesannete täitmiseks mittevajalikud) failid ja kirjad.
3.3 Teenistuja kasutajakonto, juurdepääsuõigused infosüsteemidele ja postkastile piiratakse teenistuja teenistussuhte peatumise ajaks.
3.4 Teenistussuhte peatumise lõppemisest teavitab personalitöötaja IT-spetsialisti.

4. Kasutajakonto sulgemine
4.1. Teenistussuhte lõppemisest teavitab personalitöötaja IT-spetsialisti ja kõiki infosüsteemide haldureid, kes organiseerivad teenistuja kontode sulgemise nende poolt hallatavas infosüsteemis hiljemalt teenistuja viimasele tööpäevale järgneval tööpäeval.
4.2. Teenistuja on kohustatud enne teenistussuhte lõppemist kustutama oma võrguketastelt, pilvest ja elektronpostist isiklikud (teenistusülesannete täitmiseks mittevajalikud) failid ja kirjad.
4.3. Pärast teenistussuhte lõppemist suunatakse elektronpost ajutiselt edasi uuele teenistujale või asendajale ning rakendatakse automaatvastust kuni kasutajakonto kustutamiseni.
4.4. Kasutajakonto kustutatakse kahe kuu pärast peale teenistuja teenistussuhte lõppemist. Teenistuja postkastis olevad kirjad ja pilves olevad failid on varukoopiatelt taastatavad ühe kuu jooksul alates kasutajakonto kustutamisest. Pärast seda need kustutatakse jäädavalt.

5. Riist- ja tarkvara kasutuselevõtt
5.1. Kõigi linnavalitsuse arvutivõrku püsivalt ühendatud arvutite üle peab arvestust IT-spetsialist.
5.2. Riist- ja tarkvara soetamise, paigaldamise, infosüsteemi installeerimise ja seadistamisega tegeleb ainult IT-spetsialist.
5.3. Riist- ja tarkvara ei paigaldata, kui see ei ühildu linnavalitsuse infosüsteemiga või ilmneb oht infosüsteemi toimivusele ja turvalisusele.
5.4. IT vahendid (tööjaamad, printerid, skannerid jne) paigaldatakse nii, et vastavat õigust mitteomavad inimesed ei omaks juurdepääsu konfidentsiaalsele informatsioonile ning oleks tagatud IT vahendite säilimine.

6. Paroolide reeglid
6.1. Kasutajatunnus koosneb kasutajanimest ja paroolist.
6.2. Parool peab olema vähemalt 12 tähemärki pikk või vastama kasutatava infosüsteemi nõuetele.
6.3. Parool peab sisaldama vähemalt ühte väike- (u, i, d vms) ja suurtähte (G, R, A vms) ning vähemalt ühte numbrit (5, 3, 9 vms) või erimärki (%, !, & vms). Paroolis ei tohi kasutada täpitähti (õ, ä, ö, ü).
6.4. Parool ei tohi:
    6.4.1. olla kergesti ära arvatav (näiteks kasutaja nimi, pereliikme või lemmiklooma nimi, oma telefoni- või autonumber, enda või perekonnaliikmete sünnipäev või aadress jne);
    6.4.2. sisaldada järjestikku rohkem kui kahte sama kirjamärki või sümbolit;
    6.4.3. olla samasugune kümne viimase parooliga;
    6.4.4. sarnaneda teistes IT-süsteemides kasutatavatele paroolidele;
    6.4.5. olla koostatud klaviatuurijärjestuses tähtedest või numbritest.
6.5. Kasutaja vastutab paroolide saladuses hoidmise eest ning parool tuleb sisestada teistele isikutele märkamatult. Oma isiklikku parooli ei tohi mitte kellelegi avalikustada, ka mitte IT-spetsialistile.
6.6. Kasutaja peab viivitamatult teavitama IT-spetsialisti, kui:
    6.6.1. on tekkinud kahtlus parooli teatavaks saamisest kõrvalistele isikutele;
    6.6.2. parool ununes või parool ei toimi.
6.7. Punktis 6.6. nimetatud juhtudel luuakse kasutajale uus ühekordne parool ning antakse isiklikult üle. Saadud parool tuleb ära muuta esimesel sisselogimisel.
6.8. Kasutaja kohustub arvutivõrku ja infosüsteemidesse sisenema ainult oma kasutajatunnuse ja parooliga ning tagama, et tema kasutajatunnuse abil ei pääse arvutivõrku/infosüsteemi kolmas isik ka kaugtööd tehes.
6.9. Kasutades linnavalitsuse välist seadet on paroolide salvestamine seadmesse keelatud.

6.10. Parooli ei ole lubatud ühelegi andmekandjale krüpteerimata kujul jäädvustada või dokumenteerida.
6.11. Parool vahetatakse vähemalt iga 180 päeva järel. Kui nõuet ei täideta, siis arvutivõrgu ja elektronposti kasutamise võimalus peatub.

7. Elektronposti reeglid
7.1. Iga kasutaja jaoks on tööalaselt ette nähtud nimeline elektronposti kasutajakonto. Elektronposti aadress on ette nähtud tööülesannetega seotud kirjavahetuseks.
7.2. Keelatud on tööalase elektronposti aadressi kasutamine isiklikuks kirjavahetuseks mh tarbijamängude mängimiseks, isiklike kommertsteadete tellimiseks, foorumite kasutamiseks ning muudeks tegevusteks, mis võivad põhjustada hulgalise kommertsteadete ja spämmi saatmise mõnele linnavalitsuse elektronposti aadressile.
7.3. Kasutaja ei tohi suunata tööalaseid elektronkirju automaatselt edasi välistele aadressidele.
7.4. Kasutajal on keelatud tööalase informatsiooni saatmine või vastuvõtmine kasutades selleks kolmanda osapoole elektronposti teenuseid (gmail.com, hotmail.com, hot.ee jne).
7.5. Kasutajal on keelatud linnavalitsuse elektronposti sidumine kolmanda osapoole elektronposti teenustega.
7.6. Kasutajal on keelatud avada kahtlase pealkirjaga või kahtlustäratavalt elektronposti aadressilt saabuvat elektronkirja ning käivitada elektronkirjade manuses olevaid programme või skripte. Ka esmapilgul tuntud allikatest pärit elektronkirjade puhul tuleb kontrollida, kas kirja sisu vastab oodatule ning kas manusena lisatud fail on üldse vajalik ning haakub kirja kontekstiga.
7.7. Andmete edastamiseks tuleb võimaluse korral kasutada ohutuid failiformaate ja vältida formaate, millega võidakse tahtmatult edastada kahjulikku aktiivsisu või jääkinfot. Keelatud on falitüübid: .vbs, .vbe, .scr, .reg, .jar, .exe, .docm, .app, .ani, .ace, .com, .bat, .xlsm.
7.8. Säästliku arvutivõrgu ressursside kasutamise eesmärgil on igal elektronposti kasutajal kohustus kustutada kõik ebavajalikud, sündsusetu sisuga ja viirusega nakatunud elektronkirjad.
7.9. Kasutaja elektronpostkasti sisu on varukoopiatelt taastatav 30 päeva jooksul alates kasutajakonto kustutamisest.
7.10. Elektronposti aadressi muutuse korral tuleb tagada, et üleminekuperioodi jooksul vanale aadressile saadetud kirjad oleksid kättesaadavad mitte rohkem kui üks aasta.
7.11. Elektronposti lugemiseks ja saatmiseks on lubatud kasutada ka mobiilseid seadmeid. Väljaspool linnavalitsuse sisevõrku on kasutajal ligipääs oma postkastile veebilehe kaudu. Peale veebilehitseja kasutamist tuleb postkastist välja logida ja see sulgeda.
7.12. Elektronposti kaudu ei tohi saata rämpsposti.
7.13. IT-spetsialist võib kehtestada postiloendi ja elektronposti kasutamisele täiendavaid reegleid ja piiranguid, mis ei ole vastuolus muude kehtestatud nõuetega.

8. Postiloendi ja elektronposti aliase haldamine ja reeglid
8.1. Postiloendi (meililist) või elektronposti aliase võib luua linnavalitsuse huvidest lähtuvalt juhtimise, töökorralduse, koostöö vms efektiivsemaks muutmiseks.
8.2. Postiloendi või elektronposti aliase loomiseks tuleb saata kiri IT-spetsialistile, milles on märgitud postiloendi nimi või alias, listi liikmed ja väljaspool linnavalitsust olevate liikmete elektronposti aadressid, põhjendus ja tüüp (avatud, kinnine).
8.3. Postiloend või elektronposti alias kustutakse juhul kui:
    8.3.1. selle looja avaldab selleks soovi;
    8.3.2. postiloendit ei ole kasutatud kahe aasta jooksul.
8.4. Postiloendi või aliase muutmiseks tuleb esitada põhjendatud avaldus IT-spetsialistile.

9. Printerite, skannerite ja multifunktsionaalsete seadmete kasutamine
9.1. Printerid, skannerid ja multifunktsionaalsed seadmed on mõeldud ennekõike tööga seotud dokumentide printimiseks, skaneerimiseks ja paljundamiseks.
9.2. Piiratud juurdepääsuga teavet sisaldavaid paberkandjaid on keelatud jätta seadmesse.
9.3. Dokumentide printimine mitme teenistuja poolt kasutatavast seadmest toimub teenistuja poolt määratud parooli alusel.

10. Interneti kasutamine

10.1. Interneti kasutamine töö ajal on ette nähtud ennekõike tööülesannete täitmiseks.
10.2. Kasutajal on keelatud edastada interneti kaudu (ka läbi sõnumivahetus-programmide, foorumite, blogide, kommentaaride jne) salastamata (krüpteerimata) teavet, mis on asutusesiseseks kasutamiseks mõeldud informatsioon.
10.3. Kasutajal on keelatud tundmatute ja kahtlaste failide alla laadimine või käivitamine internetist ilma IT-spetsialistiga konsulteerimata.
10.4. Kasutajal on internetis uudiseportaalide ning elektroonilise ajakirjanduse uudiste või artiklite kommenteerimine lubatud üksnes juhul, kui kasutaja teeb seda oma nime alt oma töövaldkonna kohta.

11. Kasutaja kohustused

11.1. Kasutaja on kohustatud turvalisuse tagamiseks:

11.1.1. vältima oma valduses olevate andmete ja informatsiooni lekkimist kõrvalistele isikutele;

11.1.2. töökohalt lühiajaliselt lahkudes lukustama arvuti (Win+L), pikemaks ajaks lahkudes sulgema arvuti;

11.1.3. säilitama tema kasutada antud IT vahendite riist- ja tarkvaralise komplektsuse ka väljapool linnavalitsuse tööruume;

11.1.4. kontrollima kõiki enda poolt välisel andmekandjal toodavaid või alla laaditavaid faile viirustõrje programmiga;

11.1.5 kandma hoolt arvuti välise puhtuse eest ja vajaduse korral puhastama arvutit spetsiaalsete puhastusvahenditega, mida väljastab IT-spetsialist;

11.1.6 jälgima, et arvuti ventilatsiooniavad oleksid avatud ega oleks kaetud paberite või muude esemetega;

11.1.7. vältima esemete ja vedelike sattumist arvutisse ja lisaseadmetesse;

11.1.8. võimaldama teostada tema kasutada antud IT vahendite ülevaatust ja tehnilist hooldust ning toimetama vahendid vajadusel IT-spetsialistile;

11.1.9. hoidma tööfaile arvuti töölaual (*desktop*), minu dokumentides (*my documents*), pildid (*pictures*) või OneDrive kaustas;

11.1.10. täitma muid IT-spetsialistilt saadud ühekordseid IT-alaseid korraldusi.

11.2. Kasutaja peab järgima head tava ja üldiseid eetika nõudeid ning mitte tekitama teistele kasutajatele või linnavalitsusele oma tegevusega või tegevusetusega kahju ega ohtu arvutivõrgu turvalisusele ja käideldavusele.
11.3. Turvalisuse huvides peab kasutaja võimalusel paigutama monitori selliselt, et töökohale lähenedes või aknast vaadates ei oleks ekraanil olev info kolmandatele isikutele nähtav. Kui see võimalus puudub, kasutada ekraanil oleva info kaitsmiseks spetsiaalseid turvafiltreid.

12. Kasutaja piirangud

12.1. Kasutajal on keelatud:

12.1.1. arvutivõrgu ja operatsioonisüsteemide turvaaukude, ründekoodi, paroolihäkkimise tarkvara või muu sarnase kasutamine täiendavate juurdepääsuõiguste ja privileegide saamiseks või arvutivõrgu töö häirimiseks ning teiste kasutajate kataloogide ja/või failide kustutamine või nendes olevate andmete rikkumine;

12.1.2. avada arvuti korpust, v.a IT-spetsialist;

12.1.3. paigaldada oma arvutisse tarkvara sh tööks vajalikku v.a IT-spetsialist;

12.1.4. skaneerimise, võrguliikluse pealtkuulamise või muude võrguliiklust jälgivate või segavate arvutiprogrammide või seadmete kasutamine, v.a IT-spetsialist;

12.1.5. peatada IT-spetsialisti poolt paigaldatud haldus- ja viirustõrje programme;

12.1.6. töökohustustest mittetulenev andmete eemaldamine, kustutamine, loetamatuks muutmine või üle kirjutamine;

12.1.7. kasutada autorikaitse alla kuuluvat tarkvara või andmefaile vms, mille kohta ei ole ostutõendit või muud legaalsust tõendavat dokumenti;

12.1.8. hoida arvutis riigivastase ja sündsusetu sisuga faile.

13. IT-spetsialisti kohustused ja õigused

13.1. IT-spetsialistil on kohustus:

13.1.1. tagada IT riist- ja tarkvara toimivus, turvalisus ning teenuste kättesaadavus oma tööülesannete ulatuses;
13.1.2. paigaldada teenistujatele tööks vajalik tarkvara ja uuendused;
13.1.2. teha kasutajatele kättesaadavaks arvuti, riist- ja tarkvara kasutamise juhised;
13.1.3. anda kasutajatele eelteavet olulistest muudatustest arvuti kasutamisel ning teavitama sündmustest, mis võivad mõjutada käideldavust ja privaatsust;
13.1.4. tagada tööjaama tagavarakoopiate tegemine ja säilimine, samuti vajadusel andmete taastamine;
13.1.5. hoida aktuaalselt arvutite konfiguratsiooni/standardite mudelit.

13.2. IT-spetsialistil on õigus oma töökohustuste ulatuses:
13.2.1. ajutiselt piirata hoolduse või turvalisuse huvides arvutivõrgu kasutamist;
13.2.2. jälgida arvutivõrgu toimivuse ja turvalisuse tagamiseks kõikvõimalikke võrguühendusi, lahti ühendada võrgu ülekoormust põhjustavad või pahavara levitavad seadmed;
13.2.3. nõuda kasutajatelt arvutivõrgu või -süsteemi toimivuse ja turvalisuse tagamiseks kehtestatud reeglite ning vajalike meetmete täitmist;
13.2.4. kontrollida arvutivõrgu või -süsteemi häireolukorra kiireks väljaselgitamiseks kasutajate faile.

II INFOSÜSTEEMIDE KASUTAMISE KORD

14. Infosüsteemide kasutamise kord

14.1. Infosüsteemi kasutusele võtmine toimub kooskõlastatult IT-spetsialisti ja valdkonna juhtivametnikuga.
14.2. Turvalisuse kaalutlusel on eelistatud ID (mobiil-ID, ID-kaardi, Smart-ID jms) põhised sisenemised.
14.3. Juurdepääsuõiguste ja -piirangute jagamisel järgitakse põhjendatud teadmisvajaduse põhimõtet.
14.4. Infosüsteemi kasutajaõigused saanud isikul (edaspidi *infosüsteemi kasutaja*) on õigus omada juurdepääsu talle tööks vajalikule teabele ja teenusele.
14.5. Infosüsteemi kasutaja on kohustatud:
14.5.1. kasutama infosüsteemi heaperemehelikult ja vastutustundlikult;
14.5.2. hoidma saladuses talle infosüsteemi kaudu teatavaks saanud piiratud juurdepääsuga andmeid ja teavet;
14.5.3. vältima kasutaja valduses olevate andmete ja informatsiooni lekkimist kõrvalistele isikutele;
14.5.4. koheselt teavitama infosüsteemi peakasutajat ja IT-spetsialisti kõikidest infosüsteemi häiretest, turvaintsidentidest ja ohtudest.
14.6. Infosüsteemi kasutaja vastutab enda poolt infosüsteemi sisestatavate andmete õigsuse eest.
14.7. Infosüsteemi kasutajal on keelatud linnavalitsuse infosüsteemist tööks mittevajalike väljatrükkide tegemine või sellise info kopeerimine mistahes andmekandjatele.
14.8. Kui on tekkinud kahtlus, et infosüsteemi kasutamise korda on rikutud, peatatakse infosüsteemi kasutaja juurdepääsuõigus kuni asjaolude välja selgitamiseni.
14.9. Juurdepääsuõigus suletakse kohe peale teenistussuhte lõppemist või kui selgub, et infosüsteemi kasutaja tööülesanded on muutunud selliselt, et enam ei vajata oma tööülesannete täitmiseks infosüsteemile ligipääsu.

III MOBIILSETE SEADMETE KASUTAMISE KORD

15. Mobiilsete seadmete kasutamise kord

15.1. Mobiilsete seadmete kasutamise korra eesmärk on kehtestada mobiilsete seadmete (sülearvuti, tahvelarvuti, mobiiltelefon ja teised internetivõimekusega andmetöötlust võimaldavad seadmed) kasutamise reeglid ning seeläbi kaitsta linnavalitsus arvutivõrgu ühtseid ressursse ja nende abil töödeldavaid andmeid.

15.2. Teenistusülesannete täitmiseks mobiiltelefonide soetamise, telefoninumbrite kasutamise ja kulude hüvitamise kord sätestatakse linnapea käskkirjaga.
15.3. Kasutaja peab arvestama, et seadme mobiilsus ja võimalus seadet kasutada väljaspool linnavalitsuse turvatud arvutivõrku loob suurema turvariski ning paneb kasutajale lisavastutuse.
15.4. Keelatud on jätta mobiilset seadet ilma järelevalveta üldkäidavatesse kohtadesse, sõidukitesse nähtavale kohale.
15.5. Mobiilne seade peab olema kaitstud vähemalt PIN-koodi, parooli, biomeetrilise tuvastuse või koodimustriga. Mobiiltelefoni ja tahvelarvuti lukustumine peab rakenduma automaatselt hiljemalt 1 minuti ja sülearvuti
15.8. Keelatud on asutusesiseseks puhul 5 minuti jooksul.
15.6. Mobiiltelefonides ei tohi hoida asutusesiseseks kasutamiseks tunnistatud teavet.
15.7. Andmesideprotokollid (bluetooth, wifi, hotspot) peavad olema parooliga kaitstud.
kasutamiseks mõeldud andmete edastamine ebaturvalise side kaudu (nt avalik wifi).
15.9. Linnavalitsuse poolt soetatud mobiilse seadme vargusest, kaotamisest või hävimisest on kasutaja kohustatud viivitamatult teavitama oma otsest ülemust ja IT-spetsialisti.
15.10. Vältimaks mobiilse seadme kahjustumist peab kasutaja:
15.10.1. vältima mobiilse seadme jätmist pikemaks ajaks ekstreemse temperatuuri kätte;
15.10.2. mobiilset seadet hoidma väliste kahjustuste, vedelike ja põrutuste eest kaitstuna, näiteks transportimisel hoidma seadet ettenähtud kotis/kaante vahel.
15.11. Tagamaks mobiilsetes seadmetes olevate andmete turvalisust peab kasutaja:
15.11.1. info töötlemisel veenduma, et seade on paigutatud nii, et ekraanil toimuv ei ole kolmandatele isikutele nähtav, vajadusel kasutama ekraanifiltreid;
15.11.2. väljaspool linnavalitsuse sisevõrku soovituslikult kasutama mobiilset andmesidet. Avalikes wifi võrkudes on kohustuslik kasutada krüpteeritud andmesideühendust (VPN-i);
15.11.3. kahtluse või teadmise korral, et mobiilse seadme tulemüür ja/või viirusetõrjetarkvara ei ole töökorras või on välja lülitatud või mobiilses seadmes on viirus, mitte ühendama mobiilset seadet mistahes arvutivõrku, vaid teatama juhtunust IT-spetsialisti.
15.12. Soovituslikult kasutada mobiiltelefonides tuntud tootja viirusetõrje tarkvara.
15.13. Mobiilse seadme kasutamisel dokumentide salvestamiseks või transportimiseks loetakse mobiilne seade ühtlasi väliseks andmekandjaks ja sellele kehtivad samad reeglid, mis on välja toodud punktis 16.
15.14. Mobiilsete seadmete kasutamine linnavalitsuse arvutivõrgu teenustele juurdepääsuks toimub kasutaja vastutusel ja mobiilse seadme kaudu andmete või paroolide lekkimise eest vastutab seadme omanik.
15.15. Isikliku mobiilse seadme ühendamine linnavalitsuse sisevõrku on keelatud, lubatud on kasutada külaliste wifi võrku.
15.16. Linnavalitsuse poolt soetatud mobiilse seadme esmase seadistuse teostab IT-spetsialist. Mobiilne seade antakse kasutajale kasutusse tema töökohustuste täitmiseks.
15.17. Üldjuhul kasutab mobiilset seadet üks kasutaja. Kasutajal on keelatud mobiilset seadet edasi anda kasutamiseks kolmandale isikule (k.a kasutaja pereliikmetele).
15.18. Kasutaja teenistussuhte lõppemisel tagastatakse linnavalitsuse poolt soetatud mobiilne seade linnavalitsusele.

16. Väliste digitaalsete andmekandjate kasutamise kord

16.1. Väliseks digitaalseks andmekandjaks (edaspidi *väline andmekandja*) loetakse seadmeid, millele saab salvestada digitaalset infot ja mida saab ilma tööjaama korpust avamata tööjaama küljest või arvutivõrgust eemaldada või sinna lisada (USB pulgad, mälukaardid, CD/DVD plaadid, välised kõvakettad, mobiilsed seadmed, telefonide ja fotoaparaatide mälukaardid jne).
16.2. Kasutajal on õigus saada IT-spetsialistilt väliseid andmekandjaid, kui tööülesanded seda nõuavad.
16.3. Väliste andmekandjate korral, mis ei ole linnavalitsuse poolt soetatud ja mis ühendatakse tööjaama külge, piisab IT-spetsialisti suulisest loast pärast spetsialisti veendumist, et vahend ei kujuta endast ohtu linnavalitsuse arvutivõrgu turvalisusele.
16.4. Väliste andmekandjate asemel eelistada infovahetust elektroonilist kanalit pidi. Väliste andmekandjate kasutamisel tuleb arvestada, et tegemist on kõrgendatud turvariskiga.

16.5. Kasutaja on kohustatud hoidma välist andmekandjat piisava hoolsusega, et vältida selle kadumist, kahjustumist või volitamata isikute kätte sattumist.
16.6. Asutusesiseseks kasutamiseks mõeldud informatsiooni salvestamine välisele andmekandjale on lubatud vaid otseste tööülesannete täitmiseks ning krüpteeritult.
16.7. Kui informatsiooni hoidmine andmekandjal ei ole enam otseste tööülesannete täitmiseks vajalik, tuleb informatsioon väliselt andmekandjalt kohe kustutada või andmekandja hävitada selliselt, et sellelt pole võimalik informatsiooni taastada.
16.8. Asutusesiseseks kasutamiseks mõeldud informatsiooni sisaldava andmekandja kadumisest või vargusest tuleb kohe teavitada IT-spetsialistilt.

IV INFOTURBE INTSIDENTIDE KÄSITLEMISE KORD

17. Rakendusala
17.1 Infoturbe intsidentide (edaspidi *intsident*) käsitlemise kord reguleerib intsidentidest teavitamist, nende registreerimist, lahendamist ja järelanalüüsi ning kokkuvõtte tegemist linnavalitsuse ja lepingupartnerite puhul intsidendist teavitamist.
17.2 Kui toimub isikuandmete rikkumine, siis järgitakse lisaks käesolevale korrale linna andmekaitsespetsialisti juhiseid isikuandmete kaitse üldmäärusest tuleneva rikkumisteadete esitamise korralduse kohta linnavalitsuses.
17.3. Intsidentideks loetakse muuhulgas järgmisi sündmusi: teenuse katkemine või mõne seadme rike; süsteemi tõrked või ülekoormus; inimlikud vead; mittevastavus infoturbe korra või juhenditega; füüsiliste turvameetmete rikkumine; kontrollimatud muudatused süsteemides; tarkvara või riistvara tõrked; ligipääsu rikkumised.

18. Intsidendist teavitamine
18.1 Kõik linnavalitsuse teenistujad, lepingulised töötajad ja kolmandad osapooled (edaspidi *teenistujad*) on kohustatud viivitamatult teavitama infoturbe intsidendist ja/või kahtlustest võimaliku intsidendi kohta linnavalitsuse infoturbejuhi ülesandeid täitvat IT-spetsialisti (edaspidi *IT-spetsialist*) e-posti või telefoni teel.
18.2 Intsidendist teavitamisel tuleb ilmnenud või tekkida võivat intsidenti kirjeldada võimalikult täpselt.

19. Intsidendi registreerimine ja lahendamise prioriteedi määramine
19.1 IT-spetsialist registreerib intsidendi ja määrab intsidendi lahendamise olulisuse (kriitiline, tähtis, vähe tähtis) ja korraldab intsidendi lahendamise.
19.2. Intsidendi lahendamise olulisuse tasemed on:
19.2.1. oht inimese elule ja tervisele – kriitiline intsident - oht tuleb likvideerida esmajärjekorras või kui see pole võimalik, siis maksimaalselt vähendada ohu tagajärgi inimese elule ja tervisele;
19.2.2. oht riigi sisejulgeolekule – kriitiline intsident - oht tuleb likvideerida esmajärjekorras või kui see pole võimalik, siis maksimaalselt vähendada riigi sisejulgeoleku ohustamist;
19.2.3. oht linna varale sh infovarale – kriitiline või tähtis intsident - likvideerida oht või kui see pole võimalik, siis maksimaalselt vähendada varale tekitatavat kahju;
19.2.4. oht linnavalitsuse poolt osutatavate teenuste katkemiseks – tähtis või vähetähtis - likvideerida oht ja taastada linnavalitsuse poolt osutatavad teenused võimalikult kiiresti.
19.3. Kriitilise intsidendi korral teavitab IT-spetsialist linnapead, kes on kriitilise intsidendi korral intsidendi lahendaja.
19.3.1. Teenistuja võib tema hinnangul kriitilise intsidendi korral, kui IT-spetsialistiga ei õnnestu ühendust saada, teavitada linnapead.

20. Intsidendist puutumust omavate asutuste ja isikute teavitamine
20.1 Kriitilisest ja tähtsast intsidendist teavitab IT-spetsialist 24 tunni jooksul Riigi Infosüsteemi Ameti intsidentide käsitlemise osakonda CERT-EE.
20.2 Kui intsidendist mõjutatud infosüsteemides töödeldakse isikuandmeid, teavitab IT-spetsialist juhtunust viivitamatult andmekaitsespetsialisti.

21. Intsidendi lahendamine
21.1. Intsidendi lahendaja võib infoturbe intsidendi lahendamise olulisust vajadusel muuta.
21.2. Intsidendi lahendaja peab intsidendi lahendamise olulisust muutma kohe, kui selgub, et eelnevalt määratud olulisus ei ole asjakohaselt määratud, ja vajadusel kaasama intsidendi lahendamisse vajalikke isikuid.
21.3. Saades teate intsidendi kohta, peab lahendaja hindama intsidendi lahendamiseks vajalikku aega.
21.4. IT-spetsialist on kohustatud jagama juhtnööre teenistujatele vältimaks, piiramaks ja minimeerimaks intsidendist tekkida võivaid või tekkinud kahjusid (näiteks vara väärtuse ja maine langus või isikuandmete töötlemise tagajärjel tekkiv kahju isikule).

22. Analüüs
22.1. Pärast intsidendi lahendamist kirjutab intsidendi lahendaja kokkuvõtva raporti, milles esitatakse teave tekkepõhjuste ja intsidendi lahendamise käigu kohta, nimetatakse lahendamisega seotud isikud ning tehakse ettepanekud sarnaste intsidentide vältimiseks tulevikus, sh esitatakse nimekiri meetmetest, mida eirati, rikuti või mis puudusid.
22.2. Intsidentide käsitlemise korra tõhusust testitakse kord aastas ja/või pärast iga intsidenti, pärast mille lahendamist selgus, et intsidentide korras oli vajakajäämisi.

V LÕPPSÄTTED

23. Järelevalve
Järelevalvet eeskirjast kinnipidamise üle teostavad IT-spetsialist ja linnavalitsuse juhtivametnikud.

24. Rakendussätted
24.1. Loksa linnapea 30.12.2019 käskkiri nr 2 „Loksa Linnavalitsuse arvutivõrgu ja arvutite kasutamise eeskirja kinnitamine“ tunnistatakse kehtetuks.
24.2. Juhiabil teha käesolev kord allkirja vastu teatavaks Loksa Linnavalitsuse teenistujatele.
24.3. Käskkiri jõustub 06. septembril 2023.

/allkirjastatud digitaalselt/

Värner Lootsmann
linnapea