LOKSA LINNAPEA

# K Ä S K K I R I

Loksal 20. jaanuar 2014 nr 1

**Loksa Linnavalitsuse infoturbepoliitika kinnitamine**

Võttes aluseks kohaliku omavalitsuse korralduse seaduse § 50 lg 1 p 3, avaliku teabe seaduse § 43 lg 1, Vabariigi Valitsuse 20.12.2007 määruse nr 252 „Infosüsteemide turvameetmete süsteem" § 2, annan alljärgneva

**k ä s k k i r j a:**

1. Kinnitada Loksa Linnavalitsuse infoturbepoliitika vastavalt lisale.

2. IT-spetsialist Ain Kasetalul teha Loksa Linnavalitsuse infoturbepoliitika allkirja vastu teatavaks Loksa Linnavalitsuse teenistujatele.

3. Käskkirja on võimalik vaidlustada Tallinna Halduskohtus (Pärnu mnt 7, Tallinn 15082) 30 päeva jooksul arvates teatavakstegemisest.

Värner Lootsmann
linnapea

KINNITATUD
Loksa linnapea 20.01.2014 käskkirjaga nr 1
„Loksa Linnavalitsuse infoturbepoliitika kinnitamine"
LISA

# Infoturbepoliitika

**Sisututvustus**: Infoturbepoliitika (edaspidi: *poliitika*) hõlmab Loksa Linnavalitsuse (edaspidi: *linnavalitsus*) infoturvet, sõnastades selle eesmärgid, saavutamise suunised, üldise turbekorralduse ja -strateegia ning peamiste turbemehhanismide rakendamise korra poliitikad.

Poliitika kehtestab rakendusala ulatuses varade turvalisuse tagamiseks suunised ja protseduurid, mida linnavalitsuse teenistujad on kohustatud tundma ja järgima. Poliitika on turbe eesmärkide saavutamise esmane vahend s.t kavandamise, teostuse ja halduse alus.

**Eesmärk:** infovarade kaitse, nende käideldavuse, tervikluse ja konfidentsiaalsuse tagamine.

**Kasutusulatus**: linnavalitsuse teenistujad.

**Poliitika lahutamatuteks osadeks loetakse järgmised juhendid:**
1) Loksa Linnavalitsuse arvutivõrgu ja arvutite kasutamise eeskiri
2) Võrguliikluse monitooringu kord

**Seotud dokumendid:**
Loksa Linnavalitsuse asjaajamiskord
Loksa Linnavalitsuse sisekorraeeskiri

**Mõisted:**
1. Käideldavus – infovarade kättesaadavus ja kasutatavus selleks volitatud isikutele
2. Terviklikus – veendumine, et infovarasid pole volitamata muudetud
3. Konfidentsiaalsus (salastatus) – teatud infovarade kättesaadavus ainult volitatud isikutele.

## 1. Üldsätted

Poliitika suunab infovarade haldust, kaitset ja kasutamist linnavalitsuses ning IT süsteemides. Rakendamise põhjuseks on enamike infovarade süstemaatilise kaitse vajadus, arvestades infovara spetsiifikat ja nõudeid.

Infovarade turvalisus tuleb tagada ulatuses, mis võimaldaks linnavalitsuses kõige tõenäolisemate ohtude realiseerumisel häireteta oma seadusest ja põhimäärusest tulenevaid ülesandeid täita.

Turbemeetmed peavad olema majanduslikult õigustatud ning nende rakendamisest tulenev häiriv toime linnavalitsuse tegevusele ja teenistujatele peab olema võimalikult väike.

Turvalisust puudutavate õigusaktide (sh autoriõigust, isikuandmeid, riigisaladust ja töötervishoiu, tööohutuse ja tuleohutusega seotu) täitmiseks tuleb vajadusel vastavate objektide ja protsesside puhul rakendada turvalisuse erimeetmeid.

Üldise turbemetoodika aluseks on standardid EVS-ISO/IEC TR 13335 ja EVS-ISO/IEC TR 13569. Turbemeetmete üldise metoodilise valimise, levitamise ja halduse aluseks on lähtuvalt Vabariigi Valitsuse määrusest Infosüsteemide Kolmeastmelise Etalonturbe Süsteem ISKE (http://www.riigiteataja.ee/ert/act.jsp?id=13125331).

## 2. Vastutusvaldkonnad

**Linnavalitsus**
Vastutus infotehnoloogilise turbe tagamise eest on linnapeal. Linnavalitsuse pädevusse kuuluvad turbepoliitika ja turbemeetmete väljatöötamine, kontroll meetmete täitmise üle ning vähemalt üks kord aastas turbeolukorra läbivaatuse korraldamine vajalike turbealaste muudatuste tegemiseks.

**Teenistujad**
Teenistujate valduses olevate infotehnoloogiliste varade turbe tagavad teenistujad, kellele antakse need varad kasutada tulenevalt teenistusülesannetest. Infoturbe intsidentidest (ilmnenud või oletatavatest turberiketest jms) on iga teenistuja kohustatud viivitamatult teatama linnavalitsuse IT-spetsialistile ja linnapeale. IT-spetsialist on kohustatud muuhulgas hoolitsema infovarade eest, viitama turberiskidele, neid ennetama ja lahendama turbeintsidente koostöös linnavalitsusega.

## 3. Riskianalüüs ja -haldus

**Kontroll**
Turbe vastavust poliitikale kontrollib linnavalitsus pisteliselt vähemalt üks kord kvartalis. Väline infoturbe audit tellitakse vastavalt vajadusele, kuid mitte harvemini kui üks kord kolme aasta jooksul.

**Hallatavad varad**
Linnavalitsuse tegevuse seisukohalt on oluline eeskätt alljärgnevate infovarade turvalisus, samuti andmebaaside tehnilised kirjeldused ja dokumentatsioon:

- Keskmise konfidentsiaalsusnõudega infovarad: lepingud, delikaatsed isikuandmed jms andmed, mille avalikustamine võib mõõdukalt kahjustada linnavalitsuse tegevust, usaldusväärsust, mainet ja konkurentsivõimet.
- Olulise konfidentsiaalsusega infovarad: riigisaladuse või konfidentsiaalsuslepinguga seotud lähteandmed, vahe- ja lõpptulemid.
- Personaliandmeid sisaldavad infovarad, mille puhul on oluline konfidentsiaalsus, s.h

toimikud, töölepingud, tööraamatud, palgaandmed, terviseandmed.
- Konfidentsiaalsust nõudvad töökorraldusandmeid sisaldavad infovarad: ärisaladust sisaldavate tööde detailplaanid ja täitjad, turbemehhanismide haldusandmed jms.
- Abiandmed, mille puhul on oluline käideldavus ja terviklus: taristu haldusandmed, töövahendite ja taristu dokumentatsioon.

## 4. Füüsiliste ja infovarade kaitse

Linnavalitsuses tuleb tagada järgmiste varade kaitse:
- **taristu** ehk ruumide ja tehnovõrkude turvalisus;
- **riistvara** ehk riistvaravahendite (serverite, lauaarvutite, sülearvutite, arvutite välisseadmete nagu printerite, skännerite, koopiamasinate jne ja arvutivõrgu taristu seadmete) käideldavus ja terviklus, nende tehnilised kirjeldused, infovarade dokumentatsioon;
- **sideaparatuuri** (telefoni sidesüsteem; telefonikaabelduse ja jaotusseadmete; telefonide, sh mobiiltelefonide; fakside; tulemüüride, ruuterite jm andmesideaparatuuri; andmesidekaabelduse) käideldavus ja terviklus;
- **tarkvara** ehk töökoha- ja omatarkvara käideldavus, terviklus ja legaalsus.

**Varade nimekiri**
Eelpool nimetatud infovarad, välja arvatud materjalid ja vabavara, peavad olema märgistatud, dokumenteeritud, kvantitatiivselt või kvalitatiivselt hinnatud ja kantud käibevara nimekirja, mida peavad raamatupidajad ja mille õigsust kontrollib linnavalitsus.

Varade hindamisel tuleb arvestada lisaks vara otsesele rahalisele väärtusele selle võimalikust turberikkest (hävimisest, kahjustusest, paljastusest) tulenevat kaudset kahju tööprotsesside pidurdumise, asutuse mainekahjustuste jms näol.

## 5. Turbe kavaldamine

Turbe kavandamisel, rakendamisel ja haldamisel lugeda tüüpiliste ohtude hulgas peamisteks alljärgnevad, võttes need aluseks turbemeetmete valimisel:

**Stiihilised ohud**
- tulekahju;
- vee- ja kustutuskahjustused, sh sadevee, torustike avarii jms tõttu;
- inimeksitus, nagu vilumatus, väsimus, tervisehäiretest tulenevad eksimused;
- toitekatkestus ja toite kvaliteedi kõikumine;
- riistvara tõrge;
- välise sideteenuse katkestus;
- tehnilised rikked;
- vääramatu jõud (üleujutused, äike);
- teenistujate haigestumine, lahkumine;
- elektromagnetilised häired;
- andmekandjate defektid;
- vead programmides;
- ressursinappus.

**Ründed**
- vargus;
- viirus;
- sissetung sisevõrku avalikust võrgust;
- hajus teenusetõkestus (DDoS) võrgust;

- sisemise arvutivõrgu pealtkuulamine;
- suulise suhtluse pealtkuulamine;
- teenistujate sihilikult turvalisust kahjustav käitumine;
- ründed sisevõrgust;
- andmete sihilik muutmine;
- seadmete hävitamine;
- paroolide üleandmine teistele isikutele;
- paroolide üleskirjutamine ja vale hoidmine;
- volitamata sissepääs;
- tarkvara hävitamine;
- vandalism.

## 6. Turbemeetmed

Põhiliste turbemehhanismide rakendamine ja haldus peavad vastama alljärgnevatele suunistele:

**Pääsuhaldus**
Juurdepääs ressurssidele on rollipõhine, tööalase vajaduse alusel. Tagatakse ruumide lukustamisega.

IT kasutamise rollid jaotatakse vastavalt IT-süsteemi võimalustele ja IT halduse struktuurile. Teenistujatele antakse juurdepääsu õigused vastavalt kasutajate grupile, millesse nad kuuluvad. Juurdepääs andmetele peab olema vähemalt kolmetasemeline (pääs keelatud/lugemispääs/kirjutuspääs). Kõigisse mobiilsetesse seadmetesse (arvutid, tahvelarvutid, e-lugerid, mobiiltelefonid jms), mis on teenistujate käes ja võivad sisaldada linnavalitsuse jaoks konfidentsiaalseid andmeid (e-kirjad, dokumendid, sissepääsu paroolid vms), tuleb enne seadme kasutamist ainult kasutajale teadaoleva parooli sisestamine muuta kohustuslikuks peale seadme 5 minutilist mitte aktiivset kasutamist. Kasutajate arvutite BIOS-i seadistustele ligipääs peab olema parooliga kaitstud, sealjuures operatsioonisüsteemi alglaadimise järjekord BIOS-is peab olema selline, et esmalt üritatakse sooritada alglaadimine kõvakettalt ning alles seejärel välistelt andmekandjatelt (CD/DVD, USB liidesega seade jne.).

**Paroolihaldus:**
Pääsuparoole loob ja muudab IT-spetsialist ühe tööpäeva jooksul. Süsteemi-, võrgu- jm halduse paroolidest peavad olema seifis säilitatavad kirjalikud avariieksemplarid.

Infovarade kasutajad peavad vahetama oma süsteemile juurdepääsu parooli iga 100 (saja) päeva tagant. Parooli pikkus peab olema vähemalt 8 (kaheksa) sümbolit, mis sisaldab vähemalt ühte suurt tähte, ühte väikest tähte ja ühte numbrit. Sealjuures ei tohi kasutada paroolina oma nime või ettevõtte nime või juba kasutatud paroolile sarnast parooli. Korra kasutatud parooli tohib taaskasutada mitte varem kui 2 (kahe) aasta pärast.

**Logi- ja revisjonipoliitika:**
Logid peavad võimaldama tuvastada:
- lubatavaid ja lubamatuid ressursside poole pöördumisi või pöörduskatseid, nende täpset aega ja lähtekohta;
- e-kirjade sisse- ja väljasaatmist läbi linnavalitsuse poolt kasutatava meiliserveri, sealjuures peab olema logidel ajatempliteenusega rakendatav tõestusväärtus.

Süsteemi- ja võrgulogide revisjone teeb IT-spetsialist pisteliselt vähemalt üks kord nädalas ja turbeintsidentide korral. Kõik logid tuleb talletada vähemalt üks aasta.

**Kõrvaldamispoliitika:**

Kõik tarbetud konfidentsiaalandmetega paberdokumendid tuleb hävitada paberihundis. Käibelt kõrvaldatud ja/või arhiivist säilitusaja möödumisel kõrvaldatud andmekandjad tuleb füüsiliselt hävitada.

Riigisaladusandmete ja kõrgkonfidentsiaalsete andmete kõrvaldamiseks kettalt kasutada turvalist kustutust või need kettad füüsiliselt hävitada. Kui seade on kadunud, siis võimaluse korral peab kaughalduse teel kustutama sellelt kõik linnavalitsusest puudutavad andmed ja blokeerima juurdepääsu (näiteks kaughalduse teel) linnavalitsuse poolt kasutatavale taristule seda seadet kasutades.

**Töökorralduspoliitika**
Arvutisüsteemi kasutamist reguleerib Loksa Linnavalitsuse arvutivõrgu ja arvutite kasutamise eeskiri.

**Legaalsuspoliitika**
Kõik infovarad peavad olema hangitud legaalselt. Kõik infovarade kasutusviisid peavad olema legaalsed. Tarkvara litsentside arvestust peab IT-spetsialist.

**Viirusetõrjepoliitika**
Linnavalitsuses kasutatakse viirusetõrjeks kõikidele arvutitele installeeritud residentses režiimis töötavat viirusetõrjetarkvara. Töökoha arvutite ja mobiilsete seadmete külge ühendatud väliseid andmekandjad tuleb enne kasutuselevõttu lubamist automaatselt kontrollida viirustõrje süsteemi poolt.

**Töövahendite füüsiline turve**

**Mobiilne aparatuur**
Mobiiltelefonide ja sülearvutite turbe eest vastutavad nende valdajad. IT-spetsialist on kohustatud tagama tehniliste seadistuste ja vastavate tarkvaraliste lahenduste toimimise kasutajate seadmetel ja linnavalitsuse teenistujatele kasutada antud taristul.

**Tehnoteenuste katkestused**
Serverite reservtoide peab tagama töö vähemalt viieks minutiks, puhverallikate (UPS) abil.

**Andmekandjate säilitus**
Salajase sisuga andmekandjaid tuleb säilitada seifis. Andmetega kandjaid hoitakse arhiivis (paberdokumendid), elektroonilist infot serverites. Varunduse nõuete täitmise eest vastutab IT-spetsialist. Muid olulisi andmekandjaid tuleb säilitada andmekapis.

**Töösuhte lõpetamise protseduurid**
Hiljemalt viimase tööpäeva lõpuks tuleb võtta lahkuvalt teenistujalt kõik linnavalitsuse varade pääsuvahendid (võtmed) ja -õigused (vahetada paroolid, kõrvaldada pääsuloenditest). Ülevõtmise eest vastutab vahetu ülemus. Vajadusel rakendatakse neid meetmeid vahetult pärast erakorralist töösuhte ülesütlemist.

**Pääsuõiguste vastavuse kontroll**
Kasutajate pääsuõiguste vastavust tegelikele vajadustele kontrollitakse koostöös IT-spetsialistiga vähemalt üks kord poole aasta jooksul.

## 7. Infovahetuse turve

**Võrgu taristu**
Linnavalitsuse võrgu füüsiline struktuur peab olema tsoonideks jagatud:

- serverid;

- tulemüüriga eraldatud sisemine osa;
- külalistele kasutamiseks antav wifi välisühendus, mis on tulemüüriga sisemisest võrgust.

Kogu kaabeldus (elektri-, andmeside-, telefoni-, signalisatsioonsüsteemi- jm kaabeldus) peab olema tähistatud ja dokumenteeritud ning paiknema varjatult. Kaabelduse dokumentatsioon peab sisaldama kaablite täpse asukoha hoone põhiplaanil, kaablite tehnilised andmed (mark, läbilaskevõime), kaablite markeeringu (värvus, jaotusseadmetes asuvad tähised jms.), jaotusseadmete asukoha ja tüübi ning kaablite ja jaotusseadmete paigaldus- ja parandusajad.

**Sisevõrgu haldus**
Sisevõrk on üks ja ühine kõigil linnavalitsuse teenistujatel.

**E-post**
E-posti kasutamisele esitavad detailsed nõuded on sätestatud Loksa Linnavalitsuse asjaajamiskorras ja Loksa Linnavalitsuse arvutivõrgu ja arvutite kasutamise eeskirjas.

**Faks**
Kohtvõrgu arvutites ei tohi kasutada faksmodemeid. Fakside saatmist ja vastuvõtmist kontrollib kantseleispetsialist.

**Andmevahetus salvestuskandjate abil**
Materjalide üleandmiseks kasutataval mälupulgal või laserkettal ei tohi olla mingeid muid materjale ega peitandmeid. Saadud andmekandjad tuleb enne kasutuselevõttu kontrollida viirustõrjega ja nuhkvara tõrjega. Üleantavas arvutustehnikas ei tohi olla liigseid programme ega andmeid. Üleantav tarkvara peab vastama kõigile autorikaitse- ja litsentsitingimustele.

## 8. Tegevuse katkematus

**Tagavarakoopiad, andmed ja tarkvara**
Varukoopiaid teeb IT-spetsialist linnavalitsuse töökohtade arvutitest. Varukoopiaid tehakse kataloogidest My Documents ja Desktop, sealjuures kataloogi Desktop sünkroniseeritakse varukoopiaga jooksvalt, kui arvuti paikneb linnavalitsuse sisevõrgus. Varukoopiaid ei tehta nendes kataloogides olevatest meedia failidest nagu mp3, mpeg, avi, wav. Varukoopiaid tehakse automaatselt ainult siis, kui töökohaarvuti paikneb linnavalitsuse ruumides ja on kasutaja poolt sisse logitud.

Kui varukoopia tehakse linnavalitsuse ruumides asuvasse serverisse, siis tehakse lisaks varukoopiast koopia füüsiliselt muus asukohas olevale, kuid sarnase turvalisuse astmega kohta. Varukoopiad tehakse sagedusega üks kord ööpäevas ja säilitatakse kolm kuud.

Varunduse toimimise teated tuleb saata linnavalitsuses IT eest vastutavale isikule ja IT-spetsialistile. Varunduse ja taastefunktsioonide toimimise korrektsust tuleb regulaarselt testida. Varunduse ja taastefunktsioonide juhised on toodud dokumendis „Harjumaa Omavalitsuste Liit Linnavalitsuste serverite varunduslahenduse ülesehitus".

**Riistvara varuseadmed**
Aegkriitiliste protsesside puudumise tõttu otsustatakse riistvara varuseadmete hankimise vajadus iga kord eraldi lähtuvalt olukorrast. Tööajal on lubatav riistvara seisak mitte üle 16 tunni linnavalitsuse tööjaamadele ja 8 tundi serveritele, välja arvatud stiihilistest ohtudest tekkinud seisakud. Vajadusel asendatakse rikkis riistvarakomponent ajutiselt komponendiga teisest, vähem oluliste funktsioonidega süsteemist.

## 9. Muudatuste haldus

**Turbepoliitika muutmine:**
Poliitika põhimõtted vaadatakse üle igal aastal. Poliitikat muudetakse, kui seda nõuavad turbeseire tulemused. Muudatused Poliitikas teeb linnapea. Poliitika muutmisest tingitud toimingud viiakse ellu hiljemalt ühe kuu jooksul või lähtudes muudatuste rakendamiseks koostatud aja- ja finantsgraafikust.