Kinnitatud direktori käskkirjaga

Käskkiri nr. 10-P 27.05.2019

KOHTLA – JÄRVE LASTEAED KIRJU-MIRJU

INFOTURBE JUHEND

1. Eesmärk ja üldpõhimõtted

1.1. Infoturbe juhendi eesmärgiks on reguleerida Kohtla-Järve Lasteaia Kirju-Mirju (edaspidi „lasteaed“) infotehnoloogia ala üldist korraldust, tagada infosüsteemide terviklus, konfidentsiaalsus ja käideldavus ning nende infosüsteemide organisatsiooni kooskõla kehtivate õigusaktide, tegevuskavade, standardite, protseduuride ja juhenditega.

1.2. Infotehnoloogia ala üldine korraldus asutuses peab tagama sobiva toe lasteaia eesmärkide täitmisele.

1.3. Infoturve tuleb tagada ulatuses, mis võimaldaks asutuses kõige tõenäolisemate ohtude realiseerumisel häireteta oma ülesandeid täita. Turbemeetmed peavad olema majanduslikult õigustatud ning nende rakendamisest tulenev häiriv toime asutuse tegevusele ja töötajatele peab olema võimalikult väike.

1.4. Asutuses tuleb tagada infovarade turvalisus, käideldavus ja terviklus. Kõik infovarad kirjeldatakse ülevaatuse dokumendis, mida uuendatakse kord aastas.

Infovaradeks on:

1) isikuandmed sh õpilaste, külastajate ja töötajate isikuandmed;
2) taristu: ruumid ja tehnovõrgud;
3) riistvara ehk riistvaravahendid (serverid, lauaarvutid, sülearvutid, arvutite välisseadmed nagu printerid, skännerid, koopiamasinad jms ning arvutivõrgu taristu seadmed), nende tehnilised kirjeldused, infovarade dokumentatsioon;
4) sideaparatuur (telefonikaabeldus, telefonid, sh mobiiltelefonid, tulemüürid, ruuterid, modemid jm andmesideaparatuur, andmeside kaabeldus);
5) süsteem- ja rakendustarkvara.

1.5. Turvalisust puudutavate õigusaktide (sh isikuandmete, töötervishoiu, tööohutuse ja tuleohutuse regulatsioonide) täitmiseks tuleb vajadusel vastavate objektide ja protsesside puhul rakendada turvalisuse erimeetmeid.

1.6. Turbemeetmete üldise metoodilise valimise, levitamise ja halduse aluseks on Eesti avalikus sektoris kaustatav infosüsteemide kolmeastmeline etalonturbe süsteem (ISKE, https://www.riigiteataja.ee/akt/13125331). Lisaks kasutatakse rahvusvahelist standardit ISO/IEC 27001 INFOTEHNOLOOGIA Turbemeetodid Infoturbe halduse süsteemid. Nõuded ning Center for Internet Security infoturbe raamistikku (CIS Controls, www.cisecurity.org).

(Rakendada tuleb asjakohased infoturbe meetmed, mitte valimatult mõnda nimetatuid metoodikatest).

2. IT organisatsioon

2.1. Vastutus IT ala üldise korralduse ja infoturbe tagamise eest on asutuse juhtkonnal. Juhtkond määrab infoturbe eest vastutava töötaja.

2.2. Infoturbe juhendi kujundamisel ja rakendamisel lähtutakse põhimõttest, et IT arenduse, hooldamise, kasutamise ja kontrolli funktsioonid oleksid lahus. Juhul, kui töökohustustele lahususe sisse viimine ei ole võimalik, tuleb rakendada riskide maandamiseks muid täiendavaid kontrolle. Tulenevalt asutuse organisatsiooni väiksusest võib sisuliselt võimatuks osutuda IT arenduse ja halduse lahutamine. Hooldusteenus ostetakse asjakohaselt teenusepakkujalt.

2.3. Kui infotehnoloogia-alane oskusteave ostetakse asutusse väljastpoolt, määrab juhtkond valdkonnad, kus võib kasutada edasi andmist ning kelle poolt ja kuidas edasiantud teenuseid hallatakse.

2.4. Asutus lähtub IT teenuste ostmisel järgnevatest põhinõuetest:

1) infotehnoloogia-alaste teenuste osutamise kogemus ja teenuste maht viimastel aastatel;
2) väga head teadmised infosüsteemide, arvuti riistvara, standardtarkvara, kontoritarkvara, viirustõrje vahendite ja arvutivõrgu toimimise, ülesehituse ning turvalisuse tagamise põhimõtete kohta;
3) muud nõuded, mis tulenevad eelpooltoodutest ning vastavad asutuse spetsiifikale.

2.5. Juhtkond korraldab kõigile töötajatele kord aastas infoturbe koolitused.

3. IT investeeringute juhtimine

3.1. IT halduskulude maht määratakse asutuse eelarves juhtkond.

3.2. Eelarve sisaldab riistvarainvesteeringuid, jooksvaid kulusid haldusele ja hooldamisele ning tarkvaralitsentside soetamist.

4. Riskianalüüs ja -haldus

4.1. Infotehnoloogiaga seotud riskide haldamise eest vastutab juhtkond.

4.2. Asutuse tegevuse seisukohalt on oluline eeskätt alljärgnevate infovarade turvalisus, samuti andmebaaside tehnilised kirjeldused ja dokumentatsioon:

1) keskmise konfidentsiaalsusnõudega infovarad, sh kõik isikuandmed, lepingud jms andmed, mille avalikustamine võib mõõdukalt kahjustada asutuse tegevust, usaldusväärsust, mainet ja konkurentsivõimet;
2) olulise konfidentsiaalsusega infovarad, sh konfidentsiaalsuslepinguga seotud isikuanded;
3) personaliandmeid sisaldavad infovarad, mille puhul on oluline konfidentsiaalsus, sh õpitulemused, toimikud, töölepingud, palgaandmed, terviseandmed;
4) konfidentsiaalsust nõudvad töökorraldusandmeid sisaldavad infovarad, sh ärisaladust sisaldavate tööde korraldus ja täitjad, turbemehhanismide haldusandmed;
5) abiandmed, mille puhul on oluline käideldavus ja terviklus, sh taristu haldusandmed, töövahendite ja taristu dokumentatsioon.

4.3. Asutuse infotehnoloogia riskihalduses juhindutakse järgmistest põhimõtetest:

1) kulutused IT turvalisusele ja IT teenustele peavad olema põhjendatud riski- ja tasuvuse hinnangutega;
2) riskide hindamine kaasneb iga olulise muudatusega infosüsteemides või protsessides.

4.4. Riskianalüüsi käigus selgitatakse välja võimalikud ohud ja nõrkused, hinnatakse ohtude realiseerumise tõenäosust ja nendega kaasnevaid kahjusid, valitakse sobivad meetmed ohtude realiseerumise mõju vähendamiseks, hinnatakse nende tasuvust ja otsustatakse aktsepteeritava jääkriski suurus.

4.5. Infotehnoloogilise süsteemi muutuste planeerimisel tehakse kindlaks, kas ja kuidas muutus mõjutab süsteemi ja protsessi turvalisust ning vähendatakse igakülgselt muudatustega kaasnevate riskide mõju.

5. Projektide haldus

5.1. Infotehnoloogiaga seotud projektide haldamisel lähtutakse põhimõttest, et iga olulisim arendustegevuse projekt infotehnoloogia valdkonnas peab:

1) omama täpselt määratud ja mõõdetavat eesmärki;
2) omama täpset alguse ja lõpu tähtpäeva;
3) lähtuma asutuse vajadustest.

5.2. Otsuse projektide käivitamise kohta teeb juhtkond.

5.3. Iga projekti elluviimiseks moodustatakse projektiorganisatsioon.

5.4. Projektiorganisatsioon raporteerib projekti käigust, eelarvest ja ajakavast juhtkonnale.

6. Protseduuride haldus

6.1. Infosüsteemi haldamine ja kasutamine viiakse läbi IT juhtimise parimaid praktikaid järgides.

6.2. Infosüsteemis muudatuste tegemisel muudetakse ka vastavaid protseduure ning teavitatakse kasutajaid tehtud muudatustest, kui see kasutajate andmeid puudutab.

7. Väliste teenusepakkujate kasutamine

7.1. Tegevuse edasiandmise põhimõtted

7.1.1. Asutus võib anda edasi tegevusi, mille täitmiseks kohapeal puudub ressurss või mille osutamine selleks spetsialiseerunud teenuse osutajate poolt on efektiivsem. Tegevused, mida asutus võib IT valdkonna osas anda edasi kolmandatele isikutele täielikult või osaliselt on järgmised:

1) infosüsteemide majutus ja haldus;
2) serverite majutus;
3) serverite riist- ja tarkvara hooldus ning administreerimine;
4) töökohaarvutite hooldus ja kasutajatugi;
5) võrguseadmiste ja –ühenduste hooldus;
6) tarkvara arendamine ja haldus;
7) muud tegevused asutuse juhtkonna otsuse alusel.

7.1.2. Iga konkreetse tegevuse edasiandmise ning teenuse osutaja valiku otsustab juhtkond. Juhtkond korraldab ka järelevalve üleantud tegevuste ja teenuse osutaja üle.

7.1.3. Tegevuse edasiandmise vajaduse määratlemiseks analüüsib juhtkond teenuse üleandmise vajadust ja võimalikke teenuse osutajaid, võttes arvesse punktis 7 sätestatut.

7.1.4. Analüüsi käigus tuleb keskenduda tegevuse edasiandmisega kaasnevate riskide väljaselgitamisele, leides vastused järgmistele küsimustele:

1) millised konkreetsed riskid kaasnevad tegevuse edasiandmisega?
2) milline on planeeritav tulu tegevuse edasiandmisest ja millised on tegevuse edasiandmisega seonduvad kulud?

7.1.5. Kui analüüsi tulemusena selgub, et tegevuse edasiandmine ei takista asutuse igapäevast tegevust ega kohustuste täitmist lepingupartnerite, kolmandate isikute ja pädevate ametiasutuste ees ehk tegevuse edasiandmisel ei teki olukorda, kus lepingupartnerite huvid, eriti isikuandmete osas, oleks konkreetse teenuse raames kahjustatud võrreldes

olukorraga, kus vastavaid ülesandeid täidaks asutus ise, võib juhtkond otsustada tegevuse edasiandmise.

7.2. Nõuded teenuse osutajale

7.2.1. Juhtkond korraldab teenuse osutaja suhtes põhjaliku taustauuringu, mille käigus hindab konkreetse teenuse osutaja sobivust ülesannete täitmiseks ning temaga seonduvaid riske, võttes arvesse muuhulgas teenuse osutaja ja temaga samasse konsolideerimisgruppi kuuluvate isikute kvalifikatsiooni ja tegevust, finantsseisundit, mainet ja kogemust, struktuuri ning muid sisemise töökorraldusega seonduvaid asjaolusid.

7.2.2. Teenuse osutaja valikul peab arvesse võtma järgnevat:

1) teenuse osutajal on vajalik kvalifikatsioon ning kõik õigusaktidega nõutavad load ja litsentsid ning ta on võimeline võetud kohustusi täitma ning asutusel on õigus kontrollida teenuse osutaja teenuse osutamisega seotud tegevust;
2) teenuse osutaja peab olema suuteline täitma asutusele omaseid tegevusnõudeid ja hoolsuskohustust ja tagama teenuse parima kvaliteedi;
3) teenuse osutaja reputatsioon peab olema laitmatu – teenuse osutaja ei tohi olla kriminaal- või halduskorras karistatud, arvesse tuleb võtta ka saadud trahvid, litsentsinõuete rikkumised, käimasolevate kohtuprotsesside arv ja olulisus;
4) teenuse osutaja peab olema võimeline oma kohustusi jätkusuutlikult täitma;
5) teenuse osutaja peab teostama talle edasiantud teenuse osutamise üle piisavat kontrolli ja juhtima adekvaatselt tegevusega seotud riske;
6) teenuse osutaja peab tagama konfidentsiaalse info sh isikuandmete turvalisuse, välistama huvide konfliktid ja tagama läbipaistva juhtimise;
7) teenuse osutaja tegevuse üle peab asutusel olema võimalik teostada kontrolli ja järelevalvet;
8) piiriülese teenuse pakkujaga ei tohi kaasneda riikide erinevast õigusruumist tekkivaid riske, või peavad need olema maandatud omavahelises lepingus.

7.3. Nõuded tegevuse edasiandmise lepingule

7.3.1. Tegevuse edasiandmise leping peab olema kirjalik, määratledes täpselt edasiantava tegevuse ja selle ulatuse ning sisaldama järgnevat:

1) nõuded osutavale teenusele ja teenuse osutajale ning kirjalik informeerimiskohustus tegevuse edasiandmisega seotud oluliste asjaolude muutumisest teavitamiseks;
2) asutuse juurdepääsuõigus teabele ja andmetele, mis on edasi antud ülesannete täitmisega seotud;
3) teenuse osutaja kohustus teavitada asutust viivitamatult asjaolust, mis võib oluliselt mõjutada tema võimet täita edasiantud ülesandeid nõuetekohaselt ja tulemuslikult;
4) vastutus teenuse osutaja poolsel kohustuste rikkumisel;
5) teenuse osutaja poolt kohustuste mittekohasel täitmisel rakendatavad meetmed – leppetrahvid, lepingu ennetähtaegse lõpetamise õigus asutuse poolt ilma tegevust oluliselt häirimata;
6) edasiantud tegevusega seotud ülesannete täitmiseks vajaliku ja/või ülesannete täitmisega omandatava materiaalse ja mittemateriaalse vara kuuluvus, selle kasutamise, üleandmise ja tagastamise kord ning tingimused;
7) nõuded infosüsteemidele;
8) konfidentsiaalsuskohustus ja range keeld kasutada teenuse osutamisel teatavaks saanud konfidentsiaalset teavet eesmärgipäratult (muuks otstarbeks, kui oma lepingust tulenevate kohustuste täitmiseks);
9) tagatised ja garantiid;

10) tegevuse täiendava edasiandmise nõusolek või keeld. Juhul kui tegevuse täiendav edasiandmine teenuse osutaja poolt on lubatud, siis peab asutusel säilima võimalus teostada samaväärset kontrolli edasiantud tegevuse osutamise üle;
11) lepingu muutmise, lõppemise ja lõpetamise (sealhulgas nii korralise kui ka erakorralise lõpetamise) alused, tingimused ja kord, sealhulgas õigus vajaduse korral leping lõpetada mõistliku etteteatamise tähtajaga;
12) kohustused, mida tuleb täita pärast lepingulise suhte lõppemist;
13) kohaldatav õigus ja vaidluste lahendamise kord, sh kohtualluvus;
14) tasu osutatavate teenuste eest.

7.4. **Perioodiline kontroll ja järelevalve edasiantud tegevuse ja teenuse osutaja üle**

7.4.1. Juhtkond teeb edasiantud tegevuse ja teenuse osutaja üle regulaarset kontrolli ja järelevalvet. Kontrolli tehakse vähemalt kord aastas. Kontrolli tulemused säilitatakse vähemalt 3 aastat.

7.4.2. Juhtkond vaatab vähemalt kord aastas üle osutatavate teenuste vastavuse lepingute tingimustele ja asutuse vajadustele.

8. Infovarade haldus

8.1. Juhtkond vastutab infovarade (s.h. andmed; riistavara: arvutid, serverid, võrguseadmed; litsentsid; kogu tarkvara; ka see, mille töötajad ise paigaldavad jm) üle arvestuse pidamise eest. Infovarad peavad olema dokumenteeritud, arvuliselt või kvalitatiivselt hinnatud ja kantud infovarade kaardistuse tabelisse ning isikuandmed töödeldavate isikuandmete ülevaatesse.

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

8.3. Infovarade kasutusele võtmisel lähtutakse järgmistest põhimõtetest:

1) infovara peab olema hangitud legaalselt;
2) kõik infovarade kasutusviisid peavad olema legaalsed.

8.4. Juhtkond kontrollib kord aastas infovarade nimekirja ning töökohaarvutitesse paigutatud tarkvara ja litsentsilepingute kehtivust.

9. Infoturbe kavandamine

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

<u>stiihilised ohud:</u>

- tulekahju,
- vee- ja - ja kustutuskahjustused, sh sadevee, torustike avarii jms tõttu;
- inimeksitus, nagu vilumatus, väsimus, tervisehäiretest tulenevad eksimused;
- elektrikatkestus ja elektritoite kvaliteedi kõikumine;
- riistvara tõrge;
- välise sideteenuse katkestus;
- tehnilised rikked;
- vääramatu jõud;
- töötajate haigestumine, lahkumine;
- elektromagnetilised häired;
- andmekandjate defektid,

- vead programmides;
- ressursinappus;

rünne:

- vargus;
- viirus või muu pahavara;
- sissetung sisevõrku avalikust võrgust;
- hajus teenusetõkestus (DDoS) võrgust;
- sisemise arvutivõrgu pealtkuulamine;
- suulise suhtluse pealtkuulamine;
- töötajate 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.

10. Infovarade kasutamine ja pääsuõigused

10.1. Infovarade kasutamisel lähtutakse põhimõttest, et infovarade kasutajad tuleb identifitseerida ja autoriseerida. Vastavalt infovarade tundlikkusele kehtestab juhtkond kasutajate identifitseerimise ja autoriseerimise tasemed.

10.2. Infovarade kasutajateks on: õpetajad, lapsevanemad, juhtkond, teenusepakkujad.

10.3. Kõiki õpetajaid, lapsevanemaid, juhtkonna liikmeid, teenusepakkujaid teavitatakse neile esitatavatest konfidentsiaalsusnõuetest, turvarollidest ja vastutusest. Eeldatakse, et nad on teadlikud oma kohustustest ja vastutusest infovarade infoturbe tagamisel. Juhtkond koordineerib kõiki tegevusi turvalisuse tagamiseks.

10.4. Infovarade kasutajatele, kes suhtlevad asutuse töötajatega asutuses kasutatavate infosüsteemide kaudu luuakse konto, mille kasutamise ja edastatavate andmete kasutamise kohta antakse teave asutuse andmetöötlus põhimõtteid käsitlevates dokumentides.

10.5. Õppeinfosüsteemide kasutajatele luuakse konto, mille andmeid kasutatakse vaid õppetööks ja sellega seonduvaks infovahetuseks.

10.6. Igale asutuse töötajale antakse asutuse informatsioonile juurdepääs vastavalt tema tööülesannetele.

10.7. Juurdepääsuõiguste andmisel asutuse infosüsteemis lähtutakse konkreetse töötaja tööülesannetest ning vastavale töötajale esitatavatest konfidentsiaalsusnõuetest, turvarollidest ja vastutusest, mis võivad olla täpsemalt reguleeritud:

1) juhtkonna liikme lepingus või töölepingus;
2) ametijuhendis;
3) asutuse sisekorraeeskirjades ning seda täiendavates infoturbe reeglites ja eeskirjades;
4) asutuse infoturbe koolituse materjalides.

10.8. Kasutajakontosid kaitstakse pääsuõigustega. Iga kasutaja on kohustatud oma pääsuõigusi hoidma saladuses. Pääsuõiguste kasutamisel selleks mitteautoriseeritud

isiku poolt säilib kasutajakonto omaniku vastutus kõigi tema kasutajakonto abil tehtud tegevuste eest infosüsteemides.

10.9. Pääsuõigusi kohaldatakse järgmistel juhtudel:
1) asutuse infosüsteemidele ja õpi-infosüsteemidele ligipääs;
2) töökoha, klassi või üldkasutatavale arvutile ligipääs;
3) andmesidevõrku ligipääs;
4) operatsioonisüsteemidele ligipääs;
5) rakendustele ja andmebaasidele ligipääs;
6) mobiilne- ja kaugjuurdepääs infovaradele;
7) ajutiste töötajate ja väliste kasutajate ligipääs infosüsteemile;
8) muud eelpool loetletud juhtudest tulenevad või neile sarnanevad ligipääsud.

10.10. Pääsuõiguste andmisel ja sellega seonduvas töökorralduses lähtutakse põhimõttest, et infovara kasutaja peab olema asutuse poolt piisava kindlusega tuvastatav.

10.11. Asutuse infosüsteemides kasutatavatele paroolidele kehtivad järgmised miinimumnõuded:

1) parool ei tohi olla kergesti äraarvatav (näiteks enda või asutuse nimi, auto number, sünnikuupäev, lapse nimi või muu kasutajaga seotud info või juba kasutatud paroolile sarnane parool);
2) paroolis peab olema vähemalt üks suur täht, üks väike täht ja üks number;
3) parooli pikkus peab olema vähemalt 10 märki;
4) paroole vahetatakse regulaarselt vähemalt kord aastas;
5) paroolide vahetamise käigus ei tohi uuesti kasutusele võtta juba kasutusel olnud paroole;
6) parooli turvataseme jälgimiseks peab võimalusel olema rakendatud tarkvaraline kontrollmehhanism, mis ei luba kasutajal valida nõuetele mittevastavat parooli;
7) tarkvara, seadmete jmt. tootja poolt seatud paroolid tuleb välja vahetada.

10.12. Kasutajal on paroolide kasutamisel järgnevad kohustused:
1) parooli sisestamine peab toimuma nii, et teistel isikutel ei ole võimalik sisestamise käigus tuvastada sisestatud parooli;
2) parooli ei tohi üle anda ega teatavaks teha teistele isikutele;
3) kui on teatavaks saanud paroolide sattumine teiste isikute kätte, tuleb viivitamatult vana parool välja vahetada uue vastu ja informeerida juhtunust juhtkonda;
4) paroole ja kasutajatunnuseid ei tohi edastada ebaturvaliste kanalite kaudu (elektrooniline kiri, paberile kirjutatud lahtised märkmed jne).

10.13. Süsteemi-, võrgu- ja muude halduse paroolidest (administraatori paroolid) peavad olema kirjalikud avariieksemplarid ja neid tuleb säilitada pitseeritud ümbrikes, mis on omakorda paigutatud tulekindlasse seifi.

10.14. Juhtkond kontrollib kasutajate pääsuõiguste vastavust tegelikele vajadustele vähemalt üks kord aasta jooksul.

10.15. Juhtkond võib ette näha kasutajakontode halduse täpsema korra.

11. Füüsiline turve

11.1. Olulistes ruumides peab olema paigaldatud valvesignalisatsioon ja sõlmitud valveleping turvafirmaga.

11.2. Töötajad kasutavad töös tühja laua poliitikast st töökohalt lahkudes ei ole laual liigseid dokumente. Lühiajalise lahkumise korral on arvuti kaitstud vähemalt ekraanisäästja parooliga. Tööpäeva lõpus lülitatakse arvuti välja.

11.3. Piiratud juurdepääsuga alade kaitseks kasutatakse füüsilisi (nt ruum lukustatakse) ja loogilisi juurdepääsukontrolle selliselt, et ainult volitatud isikud saavad piirkonda sissepääsu ning sellised sissepääsud fikseeritakse.

11.4. Piiratud juurdepääsuga alade puhul välditakse nende tähistamist üldarusaadavalt ja kandmist viidetele. Kogu kaabeldus (elektri-, andmeside-, telefoni-, signalisatsioonsüsteemi jm kaabeldus) peab olema tähistatud ja dokumenteeritud ning paiknema varjatult. Kaabelduse dokumentatsioon peab sisaldama kaablite täpset asukohta hoone põhiplaanil, kaablite tehnilisi andmeid (mark, läbilaskevõime), kaablite markeeringut (värvus, jaotusseadmetes asuvad tähised jms), jaotusseadmete asukohta ja tüüpi ning kaablite ja jaotusseadmete paigaldus- ja parandusaegu. Turvaliste piirkondade planeerimisel välditakse nende rajamist akendega ruumi.

11.5. Teenusepakkujate kasutamisel (nt ruumide koristus ja hooldus) rakendatakse punktis 6 toodud üldiseid ja selle teenuse jaoks asjakohaseid põhimõtteid, mis tagavad teenuseosutaja vastutuse ja asutuse varade turvalisuse.

12. Side ja operatsioonide turve

12.1. Piiratud juurdepääsuga alasid jälgitakse võimalike kahjustuste ennetamiseks ja kahjustuste korral nende kiireks avastamiseks.

12.2. Originaalandmete hävimise või riknemise vältimiseks tehakse andmetest varukoopiad.

12.3. Varukoopiaid tehakse vähemalt kord ööpäevas. Juhtkond võib määrata, millistest andmetest tuleb varukoopiaid teha tihemini. Varundamise protsessi juhib hooldusteenuse või majutuse pakkuja. Kui varukoopia tehakse asutuse ruumides asuvasse seadmesse, siis tehakse lisaks varukoopiast koopia füüsiliselt muus asukohas olevale, kuid sarnase turvalisuse astmega kohta.

12.4. Igapäevaseid varukoopiaid säilitatakse vähemalt kolm kuud. Kõikidele dokumentidele ja andmetele määratakse säilitustähtajad asjaajamise korras sõltumata, kas need on kehtestatud asjakohase seadusandlusega või on need asutuse enda kehtestada.

12.5. Varukoopiate kasutuskõlblikkust ning täielikkust kontrollitakse regulaarselt, vähemalt kord kvartalis. Varukoopia testtaastamise kohta vormistab testtaastamise läbiviija protokolli, kus on ära toodud testtaastamise aeg, taastatud andmete koosseis, testtaastamiseks kulunud aeg jt. ressursid ning testtaastamise tulemused. Testtaastamise protokollid säilitatakse ja arhiveeritakse.

12.6. Iga kriitilise infosüsteemi või andmekogu jaoks peab eksisteerima taasteplaan õnnetusjuhtumi tagajärgede kõrvaldamiseks.

12.7. Varukoopialt peab olema võimalik taastada kõikide infosüsteemide algandmed eelneva tööpäeva lõpu seisuga mistahes rikke toimumise päeval.

12.8. Juhtkond võib ette näha varundamise protsessi ja selle tehnilise toimimise täpsema korra, sealhulgas ligipääsu varukoopiatele ning andmekandjate hoidmise, säilimise ja vastutusega seonduvad küsimused.

12.9. Sülearvuti kasutajatele võimaldatakse vajaduse korral kaugligipääs asutuse infosüsteemi avalikust internetist. Kaugligipääsu võimaldamiseks kasutatakse https-ühendust ja/või samaväärseid või kõrgemaid turvameetmeid pakkuvat VPN lahendust. VPN ühendus peab olema krüpteeritud.

12.10. Sülearvutite kasutamisel väljapool asutuse ruume peab:

1) olema nendesse installeeritud operatsioonisüsteemist sõltumatu tulemüür;

2) tohib kasutada Wifi võrke, milles kasutatakse WPA või samalaadse turvalisusega juurdepääsu protokolle.

12.11. Administreerimiseks vajalik ligipääs serveritele lubatakse administreerimiseks vajalik ligipääs ka teenuse osutaja võrgust.

12.12. Asutuses kasutatakse viirusetõrjeks kõikidele arvutitele installeeritud residentses režiimis töötavat viirusetõrjetarkvara. Seadmete külge ühendatud väliseid andmekandjad tuleb enne kasutuselevõtu lubamist automaatselt kontrollida viirustõrje süsteemi poolt. Hooldusteenuse pakkuja korraldab, et viirusetõrje tarkvara oleks kaasaegne ning õigesti konfigureeritud ja võimaldaks automaatsete uuenduste paigaldamist.

12.13. Elektroonilises kirjavahetuses lähtutakse järgmistest põhimõtetest:

1) sisemine elektrooniline kirjavahetus ei tohi sattuda välisabonendile (ka tsiteerituna);
2) välisvõrku saadetud elektroonilised kirjad peavad sisaldama saatja pärisnime;
3) sisenevad ja väljuvad elektroonilised kirjad tuleb allutada automaatsele viirusekontrollile.

12.14. Sisenevates elektroonilistes kirjades on aktiivsisu (.exe, .vbs jmt) ei ole lubatud.

12.15. Võimaluse korral tuleb vältida makrosid võimaldavate vormingutega dokumentide saatmist elektroonilise kirja teel ning eelistada dokumentide saatmist pdf formaadis.

12.16. Välise osapoolega info vahetamisel lähtutakse järgmistest põhimõtetest:

1) välisele osapoolele materjalide üleandmiseks kasutataval andmekandjal ei tohi olla mingeid asjassepuutumatuid materjale ega peitandmeid;
2) välisele osapoolele üleantavas arvutustehnikas ja andmekandjatel ei tohi olla liigseid programme ega andmeid ning üleantav tarkvara peab vastama kõigile autorikaitse- ja litsentsitingimustele;
3) väliselt osapoolelt materjalide vastuvõtmisel kasutataval andmekandjal tuleb vastuvõtja poolt sooritada andmete viiruse- ja nuhkvarakontroll.

12.17. Suhtlustarkvara kasutamisel on rangelt keelatud tundmatu kontakti poolt saadetud failide vastu võtmine ja veebiviidete avamine. Enne igasuguse kontakti (ka tuntud ja usaldatud) poolt saadetud faili vastu võtmist või veebiviite avamist tuleb alati küsida saatjalt kinnitust faili või veebiviite sisu ja ohutuse kohta.

12.18. Ühegi laua- ega sülearvuti kõvakettal ei või hoida pikaajaliselt asutuse jaoks säilitamist vajavaid andmeid. Kõik tööga seotud dokumendid tuleb üldjuhul hoida välisel meedial (v.a. mälupulgad) või välistel võrguketastel.

12.19. Vajadusel rakendatakse informatsiooni kaitseks krüpteerimist. Juhtkond võib ette näha krüpteerimise rakendamise täpsema korra, näidates ära, millistel juhtudel on andmete krüpteerimine kohustuslik ning määrates kasutatava krüptograafilise algoritmi, minimaalsed krüptovõtme pikkused ja selle kuidas krüptograafilisi võtmeid hallatakse.

12.20. Välisele andmekandjale (mälupulk, laserketas) võib andmeid salvestada tagades andmete turvalisuse, kusjuures tundlikku informatsiooni sisaldavad andmeid on lubatud salvestada välisele andmekandjale ainult krüpteerituna. Kõik välised andmekandjad peavad olema märgistatud.

12.21. Kasutajate arvutite ja mobiilsete seadmete Wifi, Bluetooth ja infrapunaliidesed peavad olema välja lülitatud kui neid parasjagu ei kasutata. Tõkestatud peab olema mikrofoni ja kaamera volitamata kasutamine.

12.22. Kõigisse mobiilsetesse seadmetesse (arvutid, tahvelarvutid, e-lugerid, mobiiltelefonid jms), mis on töötajate käes ja võivad sisaldada asutuse 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).

12.23. Mobiiltelefoni on lubatud salvestada e-kirju (sünkroniseerida elektronkirja serveriga) ja muid tundlikku informatsiooni sisaldavaid andmeid ainult juhul, kui mobiiltelefoni sisu on kaitstud krüpteerimist võimaldava tarkvaraga. Kalendrikandeid on erandina lubatud salvestada (sünkroniseerida serveriga) ka mobiiltelefoni, millel krüpteerimist võimaldav tarkvara puudub.

13. Krüptokontseptsioon

13.1. Vastuvõtlikkus ohtudele ja motivatsioon.

13.1.1 Tüüpiliste ohtudeks loetakse käesolevas juhendis:

1) krüpteerimata ühenduse loomine asutuse süsteemidega ja seetõttu võimalus andmesidet pealt kuulata;
2) seadmete vargus ja sellest tulenevalt info teatavaks saamine kolmandatele osapooltele.

13.1.2. Asutust puudutavate kahjude põhjused on:

1) konfidentsiaalne info, mille avalikuks tulek võib endaga kaasa tuua kahjunõude,
2) andmed, mille avalikustamine võib kaasa tuua kellegi maine kahjustumise.

13.2. Välisvõrgust sisevõrku pöördumisel ja tundlike andmete edastamisel üldkasutatavas võrgus on kasutatakse vaid turvatud sidesessioone: VPN, SSL/HTTPS, krüpteerimine.

13.3. Sülearvutite kõvaketastel säilitatavad tundlikud andmed peavad olema krüpteeritud.

14. Arhiveerimine ja kõrvaldamispoliitika

14.1. Arhiiviväärtuslike dokumentide nimekirja määrab juhtkond
(EHIS põhimäärus § 8^1 Registri andmete säilitamine https://www.riigiteataja.ee/akt/116122016005?leiaKehtiv)

14.2. Kõik tarbetud ja säilitustähtaja ületanud konfidentsiaalandmetega paberdokumendid tuleb hävitada paberihundis asutuse vastutava töötaja poolt või usaldusväärse teenusepakkuja poolt.

14.3. Käibelt kõrvaldatud ja/või arhiivist säilitusaja möödumisel kõrvaldatud andmekandjad tuleb füüsiliselt hävitada asutuse vastutava töötaja poolt või usaldusväärse teenusepakkuja poolt.

15. Muudatuste haldus

15.1. Asutuse infosüsteemide arendamisel ja täiendamisel ning muutmisel tuleb tagada, et infosüsteemid töötlevad infot etteantud korras. Andmekvaliteeti tagatakse kontrollidega nii andmete sisestamisel kui väljundi kasutamisel.

15.2. Infosüsteemi muudatuste tagajärjel tekkida võivate õigusaktide nõuete rikkumise tõenäosuse vähendamiseks tellitakse vajadusel kavandatava muudatuse eesmärki arvestades õiguslikud analüüsid.

15.3. Kõik infosüsteemi muudatused ja arendused tuleb enne juurutamist testida.

15.4. Testimine viiakse läbi arendaja poolt selleks ettenähtud testserveris või arenduskeskkonnas. Testserveris ja arenduskeskkonnas ei kasutata tegelikke andmeid, kuid andmemahud ja nende struktuur peavad olema võrreldavad tegelikult kasutatavate andmemahtudega.

15.5. Peale kiireloomuliste muudatuste sisseviimist peab muudatuste teostaja muudatust testkeskkonnas testima ning vajadusel koostama testimisprotokolli tagantjärele.

16. Intsidentide haldus

16.1. Infoturbe rikkumiste ilmnemisel tuleb turvaintsidentidest ning probleemintsidentidest teavitada, intsidendid tuleb registreerida ning intsidendile reageerida.

16.2. Turvaintsidentideks peetakse muuhulgas järgnevaid olukordi:

1) asutuse infosüsteemidele on ligipääs isikutel, kes ei ole selleks autoriseeritud;
2) infovarade või infokandjate vargus või kadumine;
3) isikuandmete leke või tervikluse kadu;
4) tarkvara loata installeerimine või kasutamine asutuse infosüsteemides, arvutivõrgus, serverites, töökohaarvutites ja telefonides;
5) viiruse või pahavara avastamine arvutivõrgus;
6) viirusetõrje tarkvara vananemine või valesti seadistatud viirusetõrje tarkvara;
7) varukoopiate hävinemine või koopia tegemise ebaõnnestumine;
8) serverite ja töökohaarvutite turvaseadete lubamata muutmine.

16.3. Probleemintsidentideks peetakse muuhulgas järgnevaid olukordi:

1) ilmneb tarkvara viga, mis põhjustas süsteemi vigase toimimise;
2) ilmneb riistvara viga, mis põhjustas süsteemi vigase toimimise;
3) serveri seisukord põhjustab teenuse seiskumise;
4) välistest põhjustest, näiteks elektri või võrgukatkestus, tingitud teenuse seiskumine.

16.4. Töötajatel on kohustus koheselt pärast intsidendi avastamist võtta tarvitusele meetmed ohu likvideerimiseks või vähendamiseks.

16.5. Turvaintsidentidest ja probleemintsidentidest tuleb viivitamatult informeerida juhtkonda, õpetajaid, lapsevanemaid, huviringides osalejaid ning vajadusel asutuse partnereid ja pädevaid ametiasutusi.

16.6. Turvaintsidendid ja probleemintsidendid dokumenteeritakse ning infoturbejuht korraldab neile reageerimise. Intsidentide logis salvestatakse:

1) intsidendi toimumise aeg;
2) intsidendi iseloom ja mõju;
3) intsidendist teataja või avastaja;
4) tarvitusele võetud meetmed ja abinõud.

16.7. Intsidentide logikandeid säilitatakse vähemalt kolm aastat ning neid haldab juhtkond.

16.8. Juhul, kui turvaintsidendi käigus on läinud kaduma infokandja või on põhjust arvata, et asutuse konfidentsiaalne info võib olla sattunud mitteautoriseeritud isiku kätte, peab sellest koheselt teavitama juhtkonda.

16.9. Juhul, kui asutuse serverist või töökohaarvutist avastatakse turvaintsidendina käsitletavat tarkvara või viiruseid, korraldab juhtkond koos teenusepakkujatega seadme kõvaketta või mälukandja formaatimise enne seadme uuesti kasutamist.

16.10. Aegkriitiliste protsesside puudumise tõttu otsustatakse riistvara varuseadmete hankimise vajadus iga kord eraldi lähtuvalt olukorrast. Tööajal on lubatav riistvara

seisak mitte üle 16 tunni asutuse töökohtadel ja 8 tundi serveritele, välja arvatud stiihilistest ohtudest tekkinud seisakud.

16.11. Toimunud intsidente analüüsitakse vähemalt kord kvartalis, et välja selgitada nende põhjused, tuvastada puudused ja välja töötada meetmed nende puuduste likvideerimiseks ning seeläbi vältida sarnaste intsidentide kordumist tulevikus.

17. Aruandlus juhtkonnale, vastavus välisnõuetele, Infoturbe auditite vajaduse hindamine ja auditite planeerimine

17.1. Juhtkond analüüsib infoturbe seisukorda kord aastas ja ootamatult tekkivate infoturbeprobleemide korral või riskide tõttu, mis tulenevad uutest tehnilistest arengutest.

17.2. Vähemalt kord kolme aasta jooksul auditeeritakse asutust infoturbe vastavust juhendile ning kehtivatele õigusaktidele ja muudele regulatsioonidele. Auditi teeb juhtkonna poolt määratud isik või välisaudiitor. Väline infoturbe audit tellitakse vastavalt vajadusele (vajadus selgitatakse välja riskianalüüsi käigus).

17.3. Auditiaruandes kõik läbi viidud kontrolltegevused ning leitud nõuetele mittevastavused koos mittevastavuste eemaldamiseks planeeritavate tegevuste, nende eest vastutajate ning tähtaegadega. Auditi teostaja esitab auditiaruande asutuse juhtkonnale ja infoturbejuhile.

17.4. Auditi tähelepanekud ja märkused võetakse arvesse infoturbe juhtimisel ja planeerimisel. Kui auditi käigus avastatakse tõsisemaid puudusi asutuse infoturbes, tuleb peale puuduste kõrvaldamist teostada järelaudit.

18. Juhendi muutmine

18.1. Juhtkond vaatab juhendi põhimõtted üle igal aastal. Juhendit muudetakse, kui seda nõuavad turbeseire tulemused. Juhendi muutmisest tingitud toimingud viiakse ellu hiljemalt ühe kuu jooksul või lähtudes muudatuste rakendamiseks koostatud ajagraafikust.