Kinnitatud
Kohtla-Järve Lasteaed Aljonuška
direktori kt Irina Bratšun
käskirjaga 07.06.2019 nr 16-A

Kohtla-Järve
Lasteaed Aljonuška

Isikuandmete kaitse organisatsioonilised, füüsilised ja infotehnilised turvameetmed

Nõuded volitatud töötlejatele

1. ÜLDISED NÕUDED

1.1. Volitatud töötleja peab kehtestama vähemalt kõigile isikuandmeid töötlema volitatud isikutele kehtivad sisemised isikuandmete kaitse nõuded.

1.2. Volitatud töötleja peab tagama, et tema poolt isikuandmeid töötlema volitatud isikud:

1.2.1. on kohustunud järgima tähtajatut konfidentsiaalsusnõuet või nende suhtes kehtib asjakohane põhikirja- või seadusejärgne konfidentsiaalsuskohustus;

1.2.2. läbivad enne isikuandmete töötlemisega alustamist ning edaspidi vähemalt kord kahe aasta kohta infoturbe ja isikuandmete kaitse koolituse.

2. PÄÄSUÕIGUSED

2.1. Isikuandmete töötlemisel lähtutakse põhimõttest, et andmete töötlejad tuleb identifitseerida ja autoriseerida. Vastavalt infovarade tundlikkusele kehtestab juhtkond kasutajate identifitseerimise ja autoriseerimise tasemed.

2.2. Isikuandmete töötlejatele luuakse isiklik konto, mille kasutamise ja edastatavate andmete kasutamise kohta antakse teave asutuse andmetöötluse põhimõtteid käsitlevates dokumentides.

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

2.3.1. juhtkonna liikme lepingus või töölepingus;

2.3.2. ametijuhendis;

2.3.3. asutuse sisekorraeeskirjades ning seda täiendavates infoturbe reeglites ja eeskirjades;

2.3.4. asutuse infoturbe koolituse materjalides.

2.4. 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.

2.5. Pääsuõigusi kohaldatakse järgmistel juhtudel:

2.5.1. asutuse infosüsteemidele ligipääs;

2.5.2. töökoha arvutile ligipääs;

2.5.3. andmesidevõrku ligipääs;

2.5.4. operatsioonisüsteemidele ligipääs;

2.5.5. rakendustele ja andmebaasidele ligipääs;

2.5.6. mobiilne- ja kaugjuurdepääs infovaradele;

2.5.7. ajutiste töötajate ja väliste kasutajate ligipääs infosüsteemile;

2.5.8. muud eelpool loetletud juhtudest tulenevad või neile sarnanevad ligipääsud.

2.6. Asutuse infosüsteemides kasutatavatele paroolidele kehtivad järgmised miinimumnõuded:

2.6.1. 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);

2.6.2. paroolis peab olema vähemalt üks suur täht, üks väike täht ja üks number;

2.6.3. parooli pikkus peab olema vähemalt 10 märki;

2.6.4. paroole vahetatakse regulaarselt vähemalt kord aastas;

2.6.5. paroolide vahetamise käigus ei tohi uuesti kasutusele võtta juba kasutusel olnud paroole;

2.6.6. parooli turvataseme jälgimiseks peab võimalusel olema rakendatud tarkvaraline kontrollmehhanism, mis ei luba kasutajal valida nõuetele mittevastavat parooli;

2.6.7. tarkvara, seadmete jmt. tootja poolt seatud paroolid tuleb välja vahetada.

2.7. Kasutajal on paroolide kasutamisel järgnevad kohustused:

2.7.1. parooli sisestamine peab toimuma nii, et teistel isikutel ei ole võimalik sisestamise käigus tuvastada sisestatud parooli;

2.7.2. parooli ei tohi üle anda ega teatavaks teha teistele isikutele;

2.7.3. kui on teatavaks saanud paroolide sattumine teiste isikute kätte, tuleb viivitamatult vana parool välja vahetada uue vastu ja informeerida juhtunust juhtkonda;

2.7.4. paroole ja kasutajatunnuseid ei tohi edastada ebaturvaliste kanalite kaudu (elektrooniline kiri, paberile kirjutatud lahtised märkmed jne.).

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

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

3. FÜÜSILINE TURVE

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

3.2. 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.

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

3.4. 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.

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

4. SIDE JA OPERATSIOONIDE TURVE

4.1. Originaalandmete hävimise või riknemise vältimiseks tehakse andmetest varukoopiad.

4.2. Varukoopiaid tehakse vähemalt kord ööpäevas. Juhtkond võib määrata, millistest andmetest tuleb varukoopiaid teha tihemini. Kui varukoopia tehakse asutuse

ruumides asuvasse seadmesse, siis tehakse lisaks varukoopiast koopia füüsiliselt muus asukohas olevale, kuid sarnase turvalisuse astmega kohta.

4.3. 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.

4.4. 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.

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

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

4.7. Juhul kui sülearvuti kasutajatele võimaldatakse kaugligipääs asutuse infosüsteemi avalikust internetist, kasutatakse kaugligipääsu võimaldamiseks https-ühendust ja/ või samaväärseid või kõrgemaid turvameetmeid pakkuvat VPN lahendust. VPN ühendus peab olema krüpteeritud.

4.8. Sülearvutite kasutamisel väljapool asutuse ruume:

4.8.1. peab sülearvutisse olema installeeritud operatsioonisüsteemist sõltumatu tulemüür;

4.8.2. tohib kasutada vaid Wifi võrke, milles kasutatakse WPA või samalaadse turvalisusega juurdepääsu protokolle.

4.9. Viirusetõrjeks kasutatakse kõikidele arvutitele installeeritud residentses režiimis töötavat viirusetõrjetarkvara.

4.10. Seadmete külge ühendatud väliseid andmekandjad tuleb enne kasutuselevõtu lubamist automaatselt kontrollida viirustõrje süsteemi poolt.

4.11. Isikuandmeid ei tohi hoida laua- ega sülearvuti kõvakettal.

4.12. Vajadusel rakendatakse informatsiooni kaitseks krüpteerimist.

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

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

4.15. Mobiiltelefoni on lubatud salvestada e-kirju (sünkroniseerida elektronkirja serveriga) ja muid tundlikku informatsiooni (sh isikuandmeid) 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.

4.16. Eriliigilisi isikuandmeid, suures mahus isikuandmeid ning isikuandmeid, mille avalikuks saamisega võib kaasneda kahju andmesubjektile, tohib edastada vaid krüpteeritult.