PATVIRTINTA
Socialinės globos centro "Vija" direktoriaus
2024 m. kovo 21 d. įsakymu Nr.(1)-21

INFORMACIJOS IR KIBERNETINIO SAUGUMO POLITIKA

TURINYS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Informacijos ir kibernetinio saugumo politika (toliau – Politika) yra skirta pateikti vieningus ir veiksmingus Socialinio globos centro "Vija" (toliau – Įstaiga) informacijos ir kibernetinio saugumo (toliau – Saugumo) valdymo principus, Įstaigos poziciją informacijos ir kibernetinio saugumo atžvilgiu bei užtikrinti efektyvų Įstaigos informacijos ir kibernetinio saugumo valdymo proceso įgyvendinimą.

2. Pagrindinis Politikos tikslas – užtikrinti informacijos konfidencialumą, vientisumą ir prieinamumą.

3. Ši Politika privaloma visiems Įstaigos darbuotojams, laikinai dirbantiems darbuotojams ar praktiką Įstaigoje atliekantiems asmenims.

II SKYRIUS
PAGRINDINĖS SĄVOKOS

4. Pagrindiniai informacijos saugą Įstaigoje reglamentuojantys teisės aktai yra šie:

4.1. Europos Parlamento ir Tarybos 2016 m. balandžio 27 d. reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (toliau – Bendrasis duomenų apsaugos reglamentas arba Reglamentas arba BDAR);

4.2. Lietuvos Respublikos kibernetinio saugumo įstatymas;

4.3. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas;

4.4. Valstybinės duomenų apsaugos inspekcijos (toliau – VDAI arba Priežiūros institucija) „Tvarkomų asmens duomenų saugumo priemonių ir rizikos vertinimo gairės asmens duomenų valdytojams ir tvarkytojams“;

4.5. Organizacinių ir techninių kibernetinio saugumo reikalavimų aprašas.

5. Sąvokų apibrėžimai:

5.1. **Informacija** – bet koks žinių elementas, pateiktas tinkama naudoti, saugoti, perduoti ar apdoroti forma. Informacija apima žodine, rašytine, audiovizualine, skaitmenine ar bet kokia kita forma išreikštus ir apibendrintus arba interpretuotus duomenis, susijusius su Įstaiga ir/arba Įstaigos veikla, įskaitant, bet neapsiribojant, dokumentus, nuotraukas/vaizdo medžiagą, dokumentų projektus, kopijas, laiškus, schemas, planus, korespondenciją, Įstaigos studentų, tiekėjų kontaktinius duomenis.

5.2. **Informacijos saugumas (sauga)** – informacijos konfidencialumo, vientisumo ir prieinamumo užtikrinimas.

5.3. **Konfidencialumas** – informacijos savybė, užtikrinanti jos prieinamumą tik tiems fiziniams ar juridiniams asmenims (naudotojams), kuriems tokia teisė suteikta. Konfidencialios informacijos pavyzdžiai: banko sąskaitų išrašai, darbuotojų ir paslaugų gavėjų asmeninė informacija, sveikatos duomenys ir pan.

5.4. **Prieinamumas** – informacijos savybė, garantuojanti informacijos ir jos prieigai būtinų išteklių prieinamumą naudotojui reikiamu metu.

5.5. **Vientisumas** – informacijos savybė, nusakanti jos tikslumą ir pilnumo apsaugą bei užtikrinanti, kad informacija nebuvo atsitiktiniu ar neteisėtu būdu pakeista ar sunaikinta.

5.6. **Informacinių sistemų naudotojas** (toliau – Naudotojas) – Įstaigos darbuotojas ar kitas trečiasis asmuo, kuriam teisėtai suteikta prieiga prie Įstaigos informacinių išteklių.

5.7. **Informaciniai ištekliai** – informacija (duomenų bazės, duomenų rinkmenos, sutartys ir kiti dokumentai, projektinė dokumentacija, mokymų medžiaga, tęstinumo ir atkūrimo planai); programinė įranga (taikomoji ir sisteminė programinė įranga, jos kūrimo priemonės); aparatinė įranga (duomenų laikmenos, organizacinė, kompiuterinė ir ryšių įranga); informacinių technologijų ir telekomunikacijų (toliau – ITT) funkcionavimui

reikalingos paslaugos; išorės šalių teikiamos ITT paslaugos ir infrastruktūriniai ištekliai; darbuotojų kvalifikacija ir įgūdžiai.

5.8. **Informacinės sistemos** – informacijos apdorojimo sistemos ir Įstaigos išteklių (pačios informacijos, žmonių, techninių priemonių, finansų ir pan.) visuma, skirta informacijai apdoroti, formuoti (kurti), skleisti (siųsti ir gauti). Tai struktūrizuotas procesų ir procedūrų rinkinys, kuriame yra kaupiami duomenys, organizuojami ir perduodami vartotojui. Informacinėms sistemoms priklauso visos vidinės ir išorinės paslaugos, kaip interneto prieiga, elektroninis paštas, komunikacijos priemonės.

5.9. **Techninė įranga** – reiškia visą ir bet kokią Įstaigai priklausančią, techninę įrangą, įskaitant (bet neapsiribojant) kompiuterius (įskaitant personalinius, nešiojamus ir planšetinius kompiuterius), išorinius įrenginius (USB diskus ar atmintines, skaitytuvus, monitorius, klaviatūras, peles, kolonėles, ausines, mikrofonus ir pan.), periferinę įrangą (spausdintuvus, kopijavimo, skenavimo, fakso aparatus ir pan.), kompiuterių tinklo įrangą, projektorius, fotoaparatus, nepertraukiamo elektros maitinimo šaltinius, stacionarių telefonų aparatus ir pan.

5.10. **Informacijos saugumo valdymo sistema** – organizacinių ir techninių priemonių visuma, kurios tikslas yra efektyviai užtikrinti informacijos saugumą Įstaigoje.

5.11. **Informacinė aplinka** – naudotojai, organizacijos ir/arba sistemos, kurios renka, apdoroja arba platina informaciją. Taip pat, ir pati informacija.

5.12. **Kibernetinė aplinka** – informacinių sistemų naudotojai, tinklai, įrenginiai, programinė įranga, perduodama arba saugoma informacija, paslaugos ir sistemos, kurios gali būti pasiekiamos elektroniniais ryšių tinklais tiesiogiai arba netiesiogiai.

5.13. **Kibernetinis saugumas** – reiškia Įstaigos gebėjimą kibernetinėje erdvėje apsaugoti Įstaigos elektroninį ryšių tinklą, informacines sistemas bei jas apginti kibernetinių atakų atveju. Tai visuma teisinių, informacijos sklaidos, organizacinių ir techninių priemonių, skirtų kibernetiniams incidentams išvengti, juos aptikti, analizuoti ir reaguoti į juos bei įprastinei elektroninių ryšių tinklų, informacinių sistemų veiklai, įvykus šiems incidentams, atkurti.

5.14. **Kibernetinis incidentas** – vienas ar daugiau nepageidaujamų ar netikėtų informacijos saugos įvykių, turinčių faktinį neigiamą poveikį pakenkti Įstaigos veiklai ir keliančių grėsmę informacijos ir asmens duomenų saugumui.

5.15. **Incidentų valdymas** – visos procedūros, padedančios nustatyti, ištirti bei suvaldyti incidentą ir į jį reaguoti.

III SKYRIUS
POLITIKOS ĮGYVENDINIMO / UŽTIKRINIMO TIKSLAI

6. Saugi ir patikima informacinė ir kibernetinė Įstaigos aplinka, užtikrinanti aukštą elektroninių ryšių tinklų, informacinių sistemų bei informacijos saugumo lygį – tai strategiškai svarbi ir būtina sėkmingos Įstaigos veiklos ir jos tolimesnės plėtros bei Įstaigos turto ir reputacijos išsaugojimo sąlyga.

7. Pagrindiniai informacijos ir kibernetinio saugumo užtikrinimo tikslai:

7.1. užtikrinti saugią ir patikimą informacinę ir kibernetinę Įstaigos aplinką, atsižvelgiant į Įstaigos strateginius tikslus ir neviršijant Įstaigos valdomos bei prisiimamos rizikos lygio;

7.2. sudaryti sąlygas saugiai automatiniu būdu tvarkyti elektroninę informaciją;

7.3. užtikrinti Įstaigos informacijos saugumą – t. y. Įstaigos informacijos konfidencialumą, vientisumą ir prieinamumą;

7.4. užtikrinti Įstaigos veiklos tęstinumą – t. y. elektroninių ryšių tinklų, informacinių sistemų techninės bei programinės įrangos nepertraukiamą veiklą, incidentų valdymą ir savalaikį veiklos atstatymą;

7.5. ieškoti naujų būdų ir priemonių, užtikrinančių saugumą, tačiau nemažinančių patogumo naudotojams ir sistemas eksploatuojančiam personalui;

7.6. vykdyti elektroninės informacijos saugos (kibernetinių) incidentų, asmens duomenų saugumo pažeidimų prevenciją, reaguoti į elektroninės informacijos saugos (kibernetinius) incidentus, asmens duomenų saugumo pažeidimus ir juos operatyviai suvaldyti;

7.7. užtikrinti ir valdyti atitikimą, informacijos ir kibernetinį saugumą bei asmens duomenų apsaugą reglamentuojančių teisės aktų reikalavimams.

IV SKYRIUS
PAGRINDINIAI PRINCIPAI IR ĮSIPAREIGOJIMAI

8. Įstaigos informacinės ir kibernetinės aplinkos, informacinių sistemų saugumas yra užtikrinamas bei valdomas kuriant ir tobulinant vieningą saugumo sistemą, kurią sudaro teisinės, techninės, organizacinės priemonės, parenkamos siekiant valdyti riziką ir ją sumažinti iki Įstaigai priimtino rizikos lygio.

9. Įstaiga, siekdama užtikrinti informacijos ir kibernetinį saugumą, nustato šiuos informacijos ir kibernetinio saugumo valdymo principus:

9.1. **Procesinis požiūris** – saugumą užtikrinanti veikla Įstaigoje turi būti organizuojama vadovaujantis procesiniu požiūriu. Informacijos ir kibernetinio saugumo valdymo sistemos procesų rezultatai turi būti matuojami ir periodiškai vertinami, siekiant užtikrinti nepertraukiamą procesų tobulinimą ir prisitaikymą prie besikeičiančios aplinkos;

9.2. **Darna** – informacijos ir kibernetinę saugą stiprinti sistemingai užtikrinant tolygų saugumo gerinimą visose Įstaigos veiklos srityse, nuosekliai diegiant gerąsias kibernetinio saugumo praktikas ir nuolat identifikuojant bei stiprinant silpniausias saugumo sistemos grandis;

9.3. **Standartizavimas** – informacijos ir kibernetinio saugumo procedūros turi būti aiškiai reglamentuotos ir visiems žinomos, valdomos pagal nustatytą vieningą standartizuotą procesą. Diegiant ir tobulinant Saugumo procesus turi būti vadovaujamasi informacijos saugumo valdymo sistemos standarto (ISO 27001) reikalavimais ir ITIL metodika;

9.4. **Prioritetizavimas** – užtikrinant saugumą informacinėse sistemose, saugos priemonės vertinamos sekančiais aspektais, išdėstant juos prioriteto tvarka: konfidencialumas, vientisumas, prieinamumas. Saugumas sistemose įgyvendinamas prioritetus nustatant sekančiai – prieinamumas, vientisumas ir konfidencialumas;

9.5. **Klasifikavimas („Būtina žinoti“)** – visa Įstaigos informacija turi būti suskirstyta pagal konfidencialumo lygius; visa nevieša informacija aiškiai pažymėta, o jos prieiga Įstaigos personalui ir trečioms šalims suteikiama tiktai griežtai vadovaujantis principu „būtina žinoti“;

9.6. **Adekvatumas (saugumas prieš patogumą)** – apribojimai ir saugumą užtikrinančios techninės bei organizacinės priemonės diegiamos prioritetu imant saugumą, tačiau neviršijant rizikai iki Įstaigai priimtino lygio sumažinti būtinos ribos, ir užtikrinant galimybę autorizuotam Įstaigos personalui ir išorės šalims naudotis Įstaigos skaitmeninėmis paslaugomis;

9.7. **Racionalumas** – diegiami nauji įrankiai ir kitos techninės bei organizacinės priemonės, užtikrinančios saugumą bei apsaugą nuo kibernetinių grėsmių ir pažeidžiamumų, turi atitikti saugomos informacijos vertę. Jas diegiant, vadovaujantis Darnos principu, įvertinami bei panaudojami turimi Įstaigos ištekliai ir kompetencijos;

9.8. **Operatyvumas** – užtikrinamas nuolatinis informacinės ir kibernetinės aplinkos stebėjimas ir efektyvus reagavimas į kibernetinius incidentus bei informacijos ir kibernetinio saugumo incidentų (krizių) valdymas;

9.9. **Prevencija** – didesnis dėmesys turi būti skiriamas prevencijai, o ne reagavimui į incidentus ir jų pasekmes.

10. Siekdama įgyvendinti nustatytus informacijos ir kibernetinio saugumo valdymo principus, Įstaiga įsipareigoja:

10.1. skatinti ir propaguoti incidentų prevenciją užtikrinančias priemones bei visuotinės kibernetinės higienos (sąmoningumo) ir saugumo kultūrą;

10.2. skirti išteklius, būtinus nuolat planingai gerinti saugumą užtikrinančio personalo kvalifikaciją bei įgūdžius;

10.3. suteikti kompetencijas ir įgaliojimus vadovams derinti bei tvirtinti su priskirtu saugumo valdymo procesu susijusius dokumentus.

V SKYRIUS
KIBERNETINIŲ INCIDENTŲ VALDYMAS IR PREVENCIJA

11. Įstaigos funkcijos:

11.1. organizuoti ir vadovauti informacinių sistemų veiklai;

11.2. rengti ir tvirtinti teisės aktus, susijusius su duomenų sauga, ir prižiūrėti, kaip jų laikomasi;

11.3. kontroliuoti, kad informacinės sistemos būtų tvarkomos vadovaujantis Lietuvos Respublikos įstatymais ir kitais teisės aktais;

11.4. tvirtinti saugos dokumentus ir kitus teisės aktus, susijusius su informacinių sistemų elektroninės informacijos sauga (kibernetiniu saugumu) ir užtikrinti jų įgyvendinimą;

11.5. nagrinėti informacinių sistemų tvarkytojų pasiūlymus dėl informacinių sistemų elektroninės informacijos saugos (kibernetinio saugumo) tobulinimo ir priimti dėl jų sprendimus;

11.6. skirti už kibernetinių incidentų administravimą, prevenciją ir valdymą atsakingą Įstaigos vadovo įgaliotą darbuotoją (toliau – Įgaliotas darbuotojas) ir (arba) pirkti informacinių technologijų (toliau – IT) priežiūros paslaugas teikiantį išorinį paslaugos teikėją.

11.7. užtikrinti nepertraukiamą informacinės sistemos veiklą;

11.8. užtikrinti saugų elektroninės informacijos perdavimą elektroninių ryšių tinklais;

11.9. pagal kompetenciją prižiūrėti informacinės sistemos duomenų bazių valdymo sistemas, taikomųjų programų sistemas, ugniasienes, įsilaužimų aptikimo sistemas, elektroninės informacijos perdavimo tinklus ir kitus Informacinės sistemos komponentus, užtikrinti jų veikimą;

11.10. pagal kompetenciją užtikrinti informacinės sistemos elektroninės informacijos saugą (kibernetinį saugumą);

11.11. ne rečiau kaip kartą per metus organizuoti saugos dokumentų peržiūrėjimą ir aktualizavimą.

12. Įgaliotas darbuotojas, atsakingas už kibernetinių incidentų administravimą, prevenciją ir jų valdymą turi:

12.1. koordinuoti ir prižiūrėti Politikos įgyvendinimą;

12.2. teikti Įstaigos vadovui siūlymus dėl informacinių technologijų saugos atitikties vertinimo atlikimo;

12.3. teikti Įstaigos vadovui siūlymus dėl Politikos papildymo arba keitimo;

12.4. organizuoti informacinės sistemos naudotojų mokymus elektroninės informacijos saugos klausimais, informuoti juos apie elektroninės informacijos saugos problemas;

12.5. duoti informacinės sistemos naudotojams privalomus vykdyti nurodymus ir pavedimus, susijusius su Politikos įgyvendinimu;

12.6. koordinuoti elektroninės informacijos saugos (kibernetinių) incidentų tyrimą Įstaigos ir bendradarbiauti su kompetentingomis institucijomis, tiriančiomis elektroninių ryšių tinklų, informacijos saugos (kibernetinius) incidentus, neteisėtas veikas, susijusias su elektroninės informacijos saugos (kibernetiniais) incidentais;

12.7. nuolat prižiūrėti Įstaigos informacinių sistemų, tinklalapių, Įstaigos kompiuterių, tinklo veiklą;

12.8. reguliariai diegti Įstaigos informacinių sistemų, tinklalapių, Įstaigos kompiuterių, tinklo veiklai būtinus einamuosius ir saugumo atnaujinimus;

12.9. imtis visų įmanomų organizacinių, techninių ir teisinių priemonių, būtinų kibernetiniam incidentui suvaldyti ir įprastai Įstaigos veiklai atkurti;

12.10. į gautus pranešimus dėl galimų ar įvykusių kibernetinių incidentų reaguoti nedelsiant bei imtis visų reikalingų priemonių, būtinų pašalinti, sušvelninti kibernetinės atakos padarinius;

12.11. nuolat rinkti, apdoroti informaciją, susijusią su kibernetiniu incidentu ir esant būtinybei pateikti ją atitinkamoms institucijoms;

12.12. įvykus kibernetinėms atakoms apie jas informuoti Nacionalinį kibernetinio saugumo centrą;

12.13. dėl kibernetinio incidento sutrikus Įstaigos informacinių sistemų veiklai, imtis visų būtinų veiksmų, kad Įstaigos informacinių sistemų veikla būtų atkurta ir vykdoma toliau;

12.14. išaiškinus kibernetinio incidento priežastis, galimas saugumo spragas, imtis visų reikiamų priemonių, padėsiančių išvengti tokių pačių kibernetinių incidentų ateityje;

12.15. organizuoti ir vykdyti informacinių sistemų, atsarginių informacinių sistemų kopijų testavimą.

13. Įstaigos darbuotojai, pastebėję, kad prieš Įstaigos informacines sistemas, tinklalapį, Įstaigos kompiuterius, tinklus vykdoma ar įvykdyta kibernetinė ataka, nedelsiant apie tai informuoja Įstaigos įgaliotą darbuotoją, atsakingą už kibernetinių incidentų administravimą, prevenciją ir valdymą.

VI SKYRIUS
FIZINĖ APSAUGA

14. Informacijos saugai užtikrinti prieiga prie informacinių sistemų naudotojų darbo vietų yra kontroliuojama. Įstaigos serverinė yra C korpuso IV aukšte, kuri:

14.1. Uždara, 13 m2 ploto

14.2. Patalpa užrakinta, ant durų užrašas „Tarnybiniam naudojimui“

14.3. Raktą nuo patalpos saugo Įstaigos direktoriaus įsakymu paskirtas atsakingas darbuotojas, kuris:

14.3.1. Ne rečiau, kaip vieną kartą per savaitę fiziškai patikrina patalpą;

14.3.2. Nesuteikia galimybės asmenims, nesusijusiems su Įstaigos IT veikla patekti į šią patalpą

14.3.3. Nustatęs, kad yra įsilaužimo (patekimo į patalpą) požymių, nedelsiant informuoja Įstaigos direktorių

15. Taikomos C korpuso patalpų, kuriose yra Įstaigos serverinė ir C korpuso aplinkos saugumo užtikrinimo priemonės:

15.1. C korpuso įėjimas stebimas vaizdo kameromis

15.2. C korpuse, įėjus į pastatą, įėjimas stebimas budinčio individualios priežiūros darbuotojo poste.

15.3. Į C korpusą atvykstantys interesantai nukreipiami į I aukšte esančią administraciją

15.4. Įėjimai į kitas C korpuso patalpas yra užrakinti ir į jas gali patekti tik įstaigos darbuotojai, turintys raktus.

15.5. Nenaudojamos patalpos (tame tarpe ir laikinai nenaudojamos), visada rakinamos ir periodiškai patikrinamos.

16. Įstaigoje tinkamai apsaugotas fizinis perimetras - Įstaigos teritorija aptverta tvora.

17. Serverinė apsaugota nuo fizinio įsilaužimo į patalpą, prie visų C korpuso įėjimų įrengtos vaizdo kameros.

18. Komutaciniai kabeliai paslėpti kanaluose ar sienose, viešose vietose esantys lizdai užblokuoti.

19. Įstaigos lankytojas visada lydimas budinčio individualios priežiūros darbuotojo ar kito darbuotojo, kai yra tikimybė, kad lankytojas gali pamatyti konfidencialią Informaciją;

20. Įstaigos darbuotojai turėtų įsitikinti įrangą ketinančio paimti / remontuoti / konfigūruoti asmens tapatybe ir leidimu tai atlikti.

21. Darbuotojai privalo laikytis švaraus stalo principo.

22. Draudžiama į Įstaigos patalpas įnešti šiuos daiktus:

22.1. Lietuvos Respublikos Ginklų ir šaudmenų kontrolės įstatyme įrašytus visų kategorijų ginklus, jų priedėlius ir šaudmenis ar jų imitacijas;

22.2. sprogstamuosius įtaisus ir sprogiąsias medžiagas ar jų imitacijas;

22.3. narkotikus ir narkotines medžiagas bei alkoholinius gėrimus;

22.4. kitus, atvirą liepsną naudojančius ar kibirkštį skleidžiančius/sukeliančius, pavojingus daiktus, išskyrus tiesioginiam darbui, kuriam turi būti išduotas leidimas, naudojamus įrankius ar prietaisus.

23. Papildomas asmens duomenų tvarkymui taikomų saugumo priemonių sąrašas aprašytas Įstaigos Asmens duomenų tvarkymo taisyklėse.

VII SKYRIUS
REIKALAVIMAI PERSONALUI

24. Įgaliotas darbuotojas privalo išmanyti Politikos užtikrinimo principus, mokėti užtikrinti informacinių sistemų ir jose tvarkomos elektroninės informacijos saugą (kibernetinį saugumą), administruoti ir prižiūrėti informacinių sistemų komponentus (stebėti informacinės sistemos komponentų veikimą, atlikti jų profilaktinę priežiūrą, trikčių diagnostiką ir šalinimą, sugebėti užtikrinti informacinės sistemos komponentų nepertraukiamą funkcionavimą ir pan.).

25. Informacinės sistemos naudotojai privalo turėti pagrindinius darbo kompiuteriu, taikomosiomis programomis įgūdžius, mokėti tvarkyti elektroninę informaciją, būti susipažinę su Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymu, kitais teisės aktais, reglamentuojančiais asmens duomenų tvarkymą, informacinių sistemų elektroninės informacijos tvarkymą. Asmenys, tvarkantys duomenis ir informaciją, privalo laikyti jų paslaptį ir būti pasirašę Darbuotojo įsipareigojimą saugoti asmens duomenis. Darbuotojo įsipareigojimas saugoti asmens duomenis galioja ir nutraukus su elektroninės informacijos tvarkymu susijusią veiklą.

26. Informacinės sistemos naudotojų mokymo planavimo, organizavimo ir vykdymo tvarka, mokymo periodiškumo reikalavimai:

26.1. Informacinės sistemos naudotojams turi būti įvairiais būdais primenama apie elektroninės informacijos saugos (kibernetinio saugumo) problemas (pvz., priminimai elektroniniu paštu, teminių renginių organizavimas, atmintinės naujiems informacinių sistemų naudotojams ir pan.);

26.2. mokymai elektroninės informacijos saugos (kibernetinio saugumo) klausimais turi būti planuojami ir mokymo būdai parenkami atsižvelgiant į elektroninės informacijos saugos (kibernetinio saugumo) užtikrinimo prioritetines kryptis ir tikslus, įdiegtas ar planuojamas įdiegti technologijas (techninę ar programinę įrangą), informacinės sistemos naudotojų poreikius;

26.3. mokymai gali būti vykdomi tiesioginiu (pvz., paskaitos, seminarai, konferencijos ir kt. teminiai renginiai) ar nuotoliniu būdu (pvz., vaizdo konferencijos, mokomosios medžiagos pateikimas elektroninėje erdvėje ir pan.);

26.4. mokymai informacinės sistemos naudotojams turi būti organizuojami periodiškai, bet ne rečiau kaip kartą per metus. Už mokymų organizavimą atsakingas Įgaliotas darbuotojas.

26.5. mokymai Įgaliotam darbuotojui turi būti organizuojami pagal poreikį.

27. Keitimosi informacija politika ir bendros apsaugos nuo virusų taisyklės aprašytos Įstaigos Asmens duomenų tvarkymo taisyklėse.

VIII SKYRIUS
SLAPTAŽODŽIŲ NAUDOJIMAS

28. Siekiant vykdyti kibernetinių incidentų prevenciją Įstaigos darbuotojai privalo saugoti slaptažodžius, neatskleisti jų kitiems asmenims, nelaikyti matomose ir lengvai kitiems asmenims prieinamose vietose ir laikytis šių reikalavimų:

28.1. slaptažodžiai turi būti unikalūs, sudaryti iš ne mažiau kaip 8 simbolių, kuriuos sudaro mažosios raidės, didžiosios raidės, skaičiai ir specialūs simboliai;

28.2. slaptažodžiams sudaryti negalima naudoti asmeninio pobūdžio informacijos (vardų, pavardžių, gimimo datų, naminių gyvūnų vardų, kt.);

28.3. negalima naudoti kompiuterio klaviatūros sekos, pvz.: 123321, qwerty ar pan.;

28.4. kilus įtarimui, kad slaptažodis gali būti žinomas kitiems asmenims, jį būtina pasikeisti;

28.5. draudžiama keistis prisijungimo vardais, prisijungti prie informacinių išteklių, naudojantis kito naudotojo prisijungimo duomenimis;

28.6. gavus laikiną slaptažodį privaloma jį iš karto pasikeisti;

28.7. slaptažodis gali galioti ne daugiau kaip 180 dienų;

28.8. nenaudoti to paties slaptažodžio registruojantis interneto svetainėse ir Įstaigos informacinėse sistemose, kompiuteryje.

29. Prieigai prie padidinto konfidencialumo informacijos, sistemų administravimui ir privilegijuotų prieigų naudojamiems slaptažodžiams keliami papildomi reikalavimai:

29.1. slaptažodžiai turi būti sudaryti iš ne mažiau kaip 12 ženklų, parinktų atsitiktine tvarka;

29.2. neidentifikuotos prieigos turi būti apsaugotos slaptažodžiu, sudarytu iš ne mažiau kaip 12 simbolių;

29.3. slaptažodžių tvarkymui rekomenduojama naudoti slaptažodžių tvarkymo Programinę įrangą.

IX SKYRIUS
DUOMENŲ ATSARGINIS KOPIJAVIMAS

30. Atsarginis kopijavimas yra vykdomas siekiant apsaugoti Įstaigos informaciją nuo sistemos netekimo / gedimo, nuo žmogiškosios klaidos, žalingos programinės įrangos ir kt. poveikio ir leisti laiku atkurti informaciją, taip užtikrinant Įstaigos veiklos procesų tęstinumą.

31. Už Įstaigos elektroninių duomenų atsarginių kopijų darymą yra atsakingas įgaliotas darbuotojas ir (arba) IT priežiūros paslaugas teikiantis išorinis paslaugos teikėjas.

32. Įgaliotas darbuotojas ir (arba) IT priežiūros paslaugas teikiantis išorinis paslaugos teikėjas, atsakingi už reguliarų atsarginių kopijų darymą, užtikrinimą, kad jos būtų daromos nustatytu laiku ir nustatyta apimtimi privalo pasirūpinti tinkamų kontrolės priemonių, skirtų užtikrinti duomenų vientisumą kopijų atstatymo metu, diegimu. Kartą per savaitę turi peržiūrėti atsarginių kopijų ir atstatymo įrašus. Kartą per metus turi testuoti galimybę atstatyti duomenis iš atsarginių kopijų.

33. Atsarginių kopijų darymo periodiškumas ir saugojimo laikotarpis priklauso nuo informacinėje sistemoje kaupiamų elektroninių duomenų svarbos. Atsarginės duomenų kopijos turi būti daromos reguliariai ne rečiau kaip kas 1 kartą per mėnesį ir saugomos ne trumpiau kaip 1 (vienerius) metus. Atsarginės duomenų kopijos saugomos atskirai nuo duomenų.

34. Duomenų atsarginės kopijos turi būti daromos automatiniu būdu.

35. Duomenų atsarginės kopijos turi būti šifruojamos.

36. Duomenų atsarginės kopijos turi būti saugomos kitoje geografinėje vietoje nei tarnybinių stočių vieta.

37. Atsarginės kopijos turi būti apsaugotos nuo nesankcionuoto priėjimo, jų panaudojimo ar sunaikinimo.

38. Duomenys, esantys atsarginėse kopijose prieinami tik autorizuotiems naudotojams.

39. Duomenų kopijos laikomos ugniai atsparioje zonoje bei apsaugomos pagal tuos pačius saugos reikalavimus, kaip originalūs duomenys.

40. Nenaudojamos atsarginių kopijų laikmenos turi būti saugiai išvalomos ar sunaikinamos, be galimybės atkurti jose buvusius duomenis.

41. Visi veiksmai (kopijų darymo, testavimo, atstatymo, pervežimo, sunaikinimo), atliekami su atsarginėmis kopijomis, turi būti fiksuojami rašytiniuose dokumentuose.

42. Ne rečiau kaip kartą per metus atliekami informacinių sistemų duomenų atkūrimo pagal atsargines kopijas bandymai.

X SKYRIUS
MOBILIEJI, NEŠIOJAMIEJI ĮRENGINIAI

43. Mobilieji ir nešiojamieji įrenginiai, kuriais bus naudojamasi darbui su informacinėmis sistemomis, prieš naudojimąsi turi būti užregistruoti ir autorizuoti.

44. Įstaiga turi turėti galimybę nuotoliniu būdu ištrinti asmens duomenis mobiliajame, nešiojamame įrenginyje, kurio saugumas buvo sukompromituotas (pvz., pažeistos saugumo nuostatos, prarastas patikimumas).

45. Mobiliuosiuose, nešiojamuosiuose įrenginiuose turi būti atskirti privatūs ir Įstaigos veiklos duomenys, naudojant saugias programinės įrangos talpyklas (konteinerius).

46. Nenaudojami mobilieji, nešiojamieji įrenginiai turi būti fiziškai apsaugoti nuo vagystės.

47. Prieigai prie mobiliųjų, nešiojamųjų įrenginių, kuriuose dideliu mastu tvarkomi pažeidžiamų asmenų ir specialių kategorijų asmens duomenys, turėtų būti naudojamas dviejų veiksnių autentifikavimas.

48. Dideliu mastu tvarkomi pažeidžiamų asmenų ir specialių kategorijų asmens duomenys, saugomi mobiliajame įrenginyje (kaip Įstaigos duomenų tvarkymo operacijos dalis), turi būti užšifruoti.

XI SKYRIUS
INFORMACINIŲ SISTEMŲ, TECHNINĖS ĮRANGOS IR POPIERINIŲ DOKUMENTŲ NAUDOJIMAS

49. Įstaigos administracija, atsižvelgdama į Įstaigoje einamas pareigas, darbuotojams suteikia darbo priemones (kompiuterį, mobilųjį telefoną, prieigą prie interneto, elektroninį paštą, prieigą prie Įstaigos tinklo, informacinių sistemų ir programų bei kitą informacinių technologijų ir telekomunikacijų įrangą).

50. Įgaliotas darbuotojas, atsižvelgdamas su Įstaiga sudarytas sutartis bei kitų asmenų su Įstaiga sudarytus susitarimus, suteikia naudotojams prieigą prie Įstaigos kompiuterinių išteklių.

51. Suteiktos priemonės priklauso Įstaigai ir yra skirtos darbo funkcijoms vykdyti arba kitiems poreikiams, susijusiems su Įstaigos veikla.

52. Visose Įstaigos darbo vietose yra naudojamos antivirusinės priemonės, darbuotojams yra draudžiama apeiti arba išjungti antivirusinę ir/ arba apsaugos nuo kenkėjiškų programų programinę įrangą.

53. Darbuotojai neturi teisės:

53.1. savavališkai keisti techninės įrangos konfigūracijos;

53.2. savavališkai diegti, keisti, pildyti ar ištrinti programinę įrangą;

53.3. naudoti programas ar atlikti kitus veiksmus, kurie apsunkina ar trikdo kompiuterių tinklo, techninės įrangos ir/ar informacinių sistemų veikimą;

53.4. naudojantis informacinėmis sistemomis, darbuotojams griežtai draudžiama skleisti Įstaigos informaciją internete ar perduoti tokią informaciją tretiesiems asmenimis, kurie neturi teisės susipažinti su tokia informacija. Informacijos persiuntimas į savo asmeninį el. paštą, tokios informacijos nusikopijavimas asmeninėms reikmėms ar kitoks platinimas neturint Įstaigos leidimo, laikomas šiurkščiu darbo pareigų pažeidimu.

54. Darbuotojai privalo kompiuterius užrakinti, jeigu jie paliekami be priežiūros.

55. Darbuotojai turi užtikrinti techninės įrangos saugumą ir priežiūrą jei įranga išnešama iš Įstaigos patalpų.

56. Spausdinant konfidencialią ar kitą jautrią informaciją, dokumentai turi būti nedelsiant paimami nuo spausdintuvo, kad jų negalėtų perskaityti neautorizuoti asmenys.

57. Popieriniai dokumentai naikinami dokumentų naikikliu prieš juos utilizuojant.

58. Įvykus techninės įrangos ar duomenų vagystei ar praradus įrangą, darbuotojai nedelsiant turi apie tai informuoti įgaliotą darbuotoją.

XII SKYRIUS
INTERNETO, ELEKTRONINIO PAŠTO, KEIČIAMŲJŲ DUOMENŲ LAIKMENŲ NAUDOJIMAS

59. Internetas gali būti naudojamas tik esant vidiniame Įstaigos tinkle, kuris apsaugotas tinkama techninės įrangos apsauga.

60. Tiesioginė interneto prieiga naudojant modemus, mobilųjį internetą, bevielius tinklus yra draudžiama.

61. Visa informacija, programinė įranga, gauta iš interneto, turėtų būti laikoma nepatikima ir naudojama tik po patikrinimo.

62. Neleistina naudoti Įstaigos internetinį ryšį veiksmams, kurie nesuderinami su šia Politika.

63. Darbuotojas, nesilaikantis šios Politikos, yra atsakingas už visas pasekmes, kurios kyla dėl netinkamo interneto paslaugų naudojimo.

64. Įstaigos elektroninis paštas turi būti naudojamas tik darbuotojo tiesioginių pareigų vykdymui.

65. Pranešimai, pavedimai, nurodymai, informacija apie darbuotojui priskaičiuotą atlyginimą, darbuotojo prašymu teikiama informacija, informacija apie Įstaigoje galiojančių taisyklių pakeitimus ir kt. informacija naudotojams pateikiama elektroniniu paštu, išsiunčiant informaciją į jų Įstaigos elektroninio pašto dėžutes, o nesant galimybės jų įteikti Įstaigos elektroniniu paštu – į asmenines elektroninio pašto dėžutes. Esant neatidėliotinai būtinybei įvykdyti nurodymus ir pavedimus pranešimai, pavedimai, nurodymai ar kt. informacija darbuotojams gali būti perduodama skambučiu ar trumpąja žinute į Įstaigos ar asmeninį telefono numerį.

66. Elektroniniu paštu išsiųsti pavedimai yra privalomi naudotojams ir laikomi įteiktais kitą darbo dieną nuo jų išsiuntimo, jei iš naudotojo negauta patvirtinimo apie informacijos gavimą anksčiau. Skambučiu ar trumpąja žinute pavedimai ir informacija laikomi įteiktais ir privalomais skambučio metu ar trumposios žinutės išsiuntimo metu.

67. Draudžiama aktyvuoti įtartinas nuorodas gautas iš nepatikimų ir nežinomų siuntėjų.

68. Draudžiama atidarinėti el. laiškų priedus, kurie gauti iš nepatikimų siuntėjų ar atrodo įtartini, ypač su vykdomųjų bylų išplėtimais (*exe, scr, com, pif, vbs, bat* ir pan.).

69. Draudžiama kurti ar persiųsti grandininius el. paštus, kuriuose skatinama persiųsti el. laišką savo draugams ir pan.

70. Draudžiama siųsti medžiagą su trikdančia, seksualine, įžūlia, melaginga, rasistine, diskriminacine ar kita įstatymų neleidžiama informacija.

71. Draudžiama naudoti kito naudotojo el. pašto adresą.

72. Draudžiama naudoti Įstaigos el. pašto adresą asmeninių pažinčių svetainėse, elektroninėse parduotuvėse (pvz. įsigyjant prekes ar nuolaidų korteles, laisvalaikio ar su darbo funkcijomis nesusijusiose svetainėse).

73. Papildomi draudžiami veiksmai darbuotojams, naudojantiems Įstaigos elektroninį paštą, interneto prieigą ir kitą informacinių technologijų ir telekomunikacijų įrangą aprašyti Įstaigos Asmens duomenų tvarkymo taisyklėse.

74. Darbuotojui išvykstant atostogauti ar į tarnybinę komandiruotę aktyvuoti automatinio atsakymo siuntimo nustatymą.

75. Darbuotojai privalo laikytis šios darbo su keičiamųjų duomenų laikmenų, kuriose yra saugoma Įstaigos informacija ir asmens duomenys tvarkos:

75.1. jei laikmenos naudojamos duomenų perdavimui, siųsti tik per saugius kurjerius.

75.2. fiziniam skaitmeninės informacijos perdavimui, naudoti USB laikmenas, kurios yra išduotos Įstaigos;

75.3. nešiojamos laikmenos privalo būti šifruojamos jei jose yra konfidenciali informacija ir naudojamos ne Įstaigos patalpose;

75.4. nešiojamos laikmenos negali būti paliekamos be priežiūros nesaugiose vietose;

75.5. nešiojamos laikmenos neturi būti paliekamos prijungtos prie kompiuterių, kai jos nebenaudojamos;

75.6. nešiojamos laikmenos turi būti saugomos nuo dulkių, skysčių, magnetinės nuo magnetinių laukų.

75.7. leistini duomenų naikinimo būdai – perrašymas laikinais duomenimis, išmagnetinimas ir fizinis sunaikinimas. Už duomenų naikinimo organizavimą Įstaigoje atsakingas įgaliotas darbuotojas.

XIII SKYRIUS
PRIEIGOS VALDYMO REIKALAVIMAI

76. Prieiga prie Įstaigos informacinių sistemų, kuriose tvarkoma informacija ir asmens duomenys yra reguliuojama ir grindžiama reikalavimais, reikalingais atlikti tiesiogines darbo funkcijas ir siekiant apsisaugoti nuo neautorizuotos prieigos.

77. Įstaiga užtikrina, kad tik autorizuoti naudotojai pasiektų Įstaigos informacinius išteklius, kadangi neautorizuota prieiga gali įtakoti saugumo pažeidimą.

78. Prieigos teisės prie informacijos ir asmens duomenų yra suteikiamos tik autentifikuotam naudotojui, atsižvelgiant į darbuotojo pareigybę ir darbo funkcijas.

79. Visi naudotojai autentifikuojami slaptažodžiu. Įgaliotas darbuotojas išduoda trumpalaikį ir vieną kartą įvedamą slaptažodį, kurį naudotojas privalo pakeisti pirmojo prisijungimo prie informacinių sistemų metu. Išimtys gali būti patvirtintos tik įgalioto darbuotojo.

80. Pasibaigus darbo sutarties galiojimo laikui (nutraukus darbo ar paslaugų teikimo sutartį), visos su naudotoju susijusios prieigos teisės turi būti neprieinamos arba pašalintos iš informacinių sistemų.

81. Keičiantis naudotojo pareigybei, prieigos teisės turi būti peržiūrimos tiesioginio naudotojo vadovo ir po jo patvirtinimo Įgaliotas darbuotojas atitinkamai atnaujinamos prieigos teisės.

82. Įgaliotas darbuotojas periodiškai peržiūri prieigos teises (1 kartą metuose arba įvykus ženkliems sistemos pokyčiams), proceso metu peržiūrima:

82.1. neatitikimai tarp prieigos teisių suteiktų naudotojų ir aktyvių naudotojų;

82.2. neaktyvios ir nenaudojamos paskyros;

82.3. galimi piktnaudžiavimai privilegijuotomis prieigomis.

83. Draudžiama naudoti bendras naudotojų paskyras.

84. Prieiga gali būti suteikiama tik naudotojui susipažinus su Politika ir susijusiais dokumentais, siekiant įsitikinti, kad naudotojas supranta visas sąlygas.

XIV SKYRIUS
PROGRAMINĖS ĮRANGOS DIEGIMAS

85. Įstaigos darbo vietų kompiuteriai, tarnybinė stotis, mobilieji ir kiti įrenginiai bei tinklo įranga, turi įdiegtus naujausius operacinės sistemos atnaujinimus.

86. Atnaujinimų diegimą ir priežiūrą vykdo Įgaliotas darbuotojas.

87. Antivirusinėje apsaugos sistemoje nustatytas automatinis virusų ir kenkėjiškų programų virusų žodynų atsisiuntimas.

88. Naudojami automatiniai atnaujinimo valdymo įrankiai, užtikrinant naujausius kompiuterinės programinės įrangos ar operacinių sistemų atnaujinimus iš gamintojų.

89. Teikėjų teikta programinė įranga palaikoma naujausia gamintojo paskelbta versija.

90. Programinė įranga diegiama po sėkmingo išbandymo.

XV SKYRIUS
IŠTEKLIŲ IR TURTO VALDYMAS

91. Visi Informaciniai ištekliai gali būti naudojami Įstaigos veiklos funkcijoms atlikti.

92. Darbuotojai informacinius išteklius naudoja laikydamiesi šios Politikos, teisės aktų reikalavimų, licencinių ar kitų sutarčių nuostatų bei techninės įrangos eksploatavimo taisyklių.

93. Darbuotojai, Įstaigos įgalioti atlikti informacijos saugos ir informacinių išteklių priežiūrą gali bet kuriuo metu tikrinti techninės ir programinės įrangos darbą, kompiuterio tinklo srautą ir naudotojų veiksmus Įstaigos informacinėse sistemose.

94. Draudžiama veikla:

94.1. Draudžiama naudoti techninę ir programinę įrangą būdais, kurie:

- sukelia saugumo grėsmes;
- užima resursus be reikalo;
- mažina sistemos greitaveiką.

94.2. mėtyti, laužyti, daužyti, ardyti įrenginius;

94.3. bandyti apeiti, šalinti ar išjungti įrenginyje nustatytas saugos priemones;

94.4. naudoti nelicencijuotą programinę įrangą ar kitą intelektualią nuosavybę;

94.5. neleistinai kopijuoti autorių teisių saugomą turinį;

94.6. siųstis informaciją, kuri nėra skirta Įstaigos tikslams pasiekti, pvz., nuotraukas, vaizdo medžiagą, programinę įrangą;

94.7. diegti ir žaisti žaidimus, siųsti grandininius elektroninius laiškus;

94.8. diegti ir/ar naudoti programinę įrangą, kuri nėra Įstaigos patvirtintos programinės įrangos sąraše, tame tarpe Java/ActiveX priedėlius, programas išorinėse laikmenose;

94.9. naudoti informacijos ar sesijos šifravimo įrankius, nebent tai būtų nustatyta Įstaigos politikose ar tvarkose;

94.10. diegti ir naudoti periferinius įrenginius, kaip modemai, tinklo kortos, atminties kortelės ar kiti atminties įrenginiai (pvz., USB diskai, fotoaparatai, kt.) be Įgalioto darbuotojo leidimo;

94.11. keistis prisijungimo duomenimis ir prisijungti prie informacinių išteklių pasinaudojus kito naudotojo prisijungimo duomenimis;

94.12. naudoti Įstaigos informacinius išteklius kuriant ar perduodant žiaurius; įžeidžiančio, pornografinio ar panašaus turinio informaciją;

94.13. draudžiama jungtis prie Įstaigos kompiuterinių tinklų, naudojantis asmenine technine įrangą.

94.14. negalima vykdyti veiklos pažeidžiančios Lietuvos Respublikos ir tarptautinius teisės aktus;

94.15. negalima pažeisti asmenų privatumo teisės.

XVI SKYRIUS
NUOTOLINIO DARBO SAUGUMO REIKALAVIMAI

95. Darbuotojams prisijungti prie Įstaigos vidinio tinklo ir dirbti nuotoliniu būdu galima tik gavus Įgalioto darbuotojo leidimą. Jungiantis nuotoliniu būdu, naudotojai turi būti autorizuoti ir prisijungimas galimas tik naudojant šifruotus ryšio kanalus.

96. Nuotolinio ryšio sujungimas ir nuotolinės prieigos suteikimas vyktų vadovaujantis principu *„Būtina darbui / būtina žinoti“* bei turėtų sutartą galiojimo terminą.

97. Draudžiama leisti naudotis įranga, skirta nuotoliniam darbui, naudotis tretiesiems asmenims.

98. Dirbant nuotoliniu būdu, turi būti pasirinkta pakankamai saugi fizinė aplinka, kurioje nebūtų galima atskleisti konfidencialios ir vidinės informacijos neautorizuotiems asmenims, tame tarpe ir šeimos nariams ar draugams.

99. Paliekant įrangą neprižiūrimą, ji turi būti paliekama saugiai (žmonių keliamos, aplinkos keliamos grėsmės), užtikrinant jos ir joje esančios informacijos saugumą. Negalima prie įrangos jungti neautorizuotos įrangos, diegti programinės įrangos.

100. Nuotoliniu būdu dirbančių darbuotojų įranga turi atitikti Įstaigos nustatytus nuotolinės įrangos standartus (įdiegtos ir atnaujintos antivirusinės programos, sudiegti visi naudojamos programinės įrangos atnaujinimai, įjungta ugniasienė ir pan., ekrano užsklandos įsijungimo laikas ir pan.).

101. Draudžiama jungtis prie nepatikimų (įvertinama paties naudotojo) *WiFi* ar kt. tinklų.

102. Draudžiama naudoti nuotolinę prieigą jei nenaudojamas Saugus VPN ryšys.

103. Išnešama iš Įstaigos aplinkos techninė įranga su informacija užšifruota.

104. Visa informacija, sukurta nuotoliniu būdu, yra Įstaigos nuosavybė.

XVII SKYRIUS
DUOMENŲ NAIKINIMAS, ŠALINIMAS

105. Prieš pašalinant bet kokią duomenų laikmeną turi būti sunaikinti visi joje esantys duomenys. Jei to padaryti neįmanoma (pvz., DVD laikmenos), turi būti įvykdytas fizinis duomenų laikmenos sunaikinimas be galimybės atstatyti.

106. Popierinės ir nešiojamosios duomenų laikmenos (pvz., DVD laikmenos), kuriose buvo saugomi, kaupiami asmens duomenys, turi būti naikinamos tam skirtais smulkintuvais arba kitomis mechaninėmis priemonėmis.

107. Jei būtina, prieš šalinant laikmenas, turi būti atlikti visų šalinamų laikmenų daugybiniai programinės įrangos perrašymai (angl. *Multiple passes of softwarebased overwriting*).

108. Jei saugiems duomenų naikinimo ir šalinimo duomenų laikmenose ar popieriniuose dokumentuose darbams atlikti yra pasitelkiamos trečiosios šalies paslaugos, turi būti sudaryta atitinkama paslaugų sutartis ir atliekamas sunaikintų įrašų protokolavimas.

109. Po dideliu mastu tvarkomų pažeidžiamų asmenų ir specialių kategorijų asmens duomenų ištrynimo, reikėtų imtis papildomų priemonių, pvz., gali būti atliktas nepageidaujamos magnetinės informacijos pašalinimas (išmagnetinimas). Priklausomai nuo konkretaus atvejo reikėtų įvertinti fizinio sunaikinimo galimybes.

110. Kiek tai liečia pažeidžiamų asmenų ar specialių kategorijų asmens duomenų tvarkymą dideliu mastu, jei saugiems įrašų naikinimo ir šalinimo duomenų laikmenose ar popieriniuose dokumentuose darbams atlikti yra pasitelkiamos trečiojo asmens paslaugos, turi būti užtikrinta, kad šis procesas vyktų Įstaigos patalpose, siekiant išvengti asmens duomenų perdavimo tretiesiems asmenims. Atskirais atvejais, kai to neįmanoma atlikti Įstaigos patalpose, sunaikinimas gali būti atliekamas kitoje fizinėje vietoje, tačiau tik stebint Įgaliotam Įstaigos darbuotojui.

XVIII SKYRIUS
VEIKLOS TĘSTINUMO VALDYMAS

111. Įstaigoje yra patvirtintas „Veiklos tęstinumo planas“, kuriame nustatyta tvarka, kurios reikia laikytis kritinės situacijos, kad būtų užtikrintas informacinių išteklių prieinamumas ir Įstaigos veiklos tęstinumas.

112. Veiklos tęstinumo plano veiksmingumas tikrinamas kiekvienais kalendoriniais metais, imituojant kritines situacijas, jų metu paskirti atsakingi asmenys atlieka kritinės situacijos veiksmus apibrėžtus dokumente „Veiklos tęstinumo planas“. Pastebėti trūkumai ir pažeidžiamumai analizuojami ir nustatomos gerinimo priemonės.

XIX SKYRIUS
POLITIKOS ĮGYVENDINIMAS IR KONTROLĖ

113. Informacijos saugos ir asmens duomenų saugos mokymai turi būti organizuojami ne rečiau kaip kartą per kalendorinius metus arba dažniau, jeigu yra poreikis, įtraukiant naujus Įstaigos darbuotojus.

114. Darbuotojai pradėdami eiti savo pareigas, turi būti pasirašytinai supažindinti su Įstaigos Politika, taip pat pasirašyti atitinkamus informacijos konfidencialumo ir neatskleidimo susitarimus (Darbuotojo įsipareigojimas saugoti asmens duomenis).

115. Politika ne rečiau kaip kartą per metus peržiūrima ar tinkamai įgyvendinama praktikoje, ir esant poreikiui parengiami bei pateikiami pasiūlymai dėl šios Politikos pakeitimų.

PATVIRTINTA
Socialinės globos centro "Vija" direktoriaus
2024 m. kovo 21 d. įsakymu Nr. (1)-21

INFORMACINIŲ SISTEMŲ VEIKLOS TĘSTINUMO VALDYMO PLANAS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Socialinio globos centro "Vija" (toliau – Įstaiga) informacinių sistemų veiklos tęstinumo valdymo plano (toliau – Valdymo planas) tikslas – nustatyti Įstaigos informacinių sistemų naudotojų ir kitų asmenų veiksmus, esant elektroninės informacijos saugos incidentui, kurio metu iškyla pavojus informacinių sistemų duomenims, techninės, programinės įrangos funkcionavimui.

2. Vartojamos sąvokos:

2.1. **Įstaigos informacinės sistemos** (toliau – Informacinės sistemos) – informacinių technologijų pagrindu veikiančios sistemos, užtikrinančios kompiuterizuotą Įstaigos duomenų, dokumentų ir kitos informacijos kūrimą, tvarkymą ir saugojimą, tenkinančios kitus Įstaigos informacinius poreikius. Informacines sistemas sudaro techninė įranga (tarnybinės stotys, darbo vietų kompiuteriai, duomenų saugyklos, kompiuterių tinklo ir elektroninio ryšio priemonės, duomenų apsaugos priemonės), programinė įranga (operacinės sistemos, pagalbinės programos, taikomosios programinės įrangos), kompiuterizuotai tvarkoma Įstaigos veiklos informacija (elektroniniai dokumentai, įvairūs duomenys, duomenų bazės) ir kita informacija;

2.2. **Kritinė situacija** – informacijos saugos incidentas, dėl kurio sutrinka ar gali sutrikti pagrindiniai Įstaigos veiklos procesai.

2.3. **Informacinių sistemų naudotojas** (toliau – Naudotojas) – Įstaigos darbuotojas ar kitas trečiasis asmuo, kuriam teisėtai suteikta prieiga prie Įstaigos informacinių išteklių.

2.4. **Informacijos saugos incidentas** – vienas ar daugiau nepageidaujamų ar netikėtų įvykių, turinčių didelę tikimybę pakenkti Įstaigos veiklai ir keliančių grėsmę informacijos ir asmens duomenų saugumui.

3. Valdymo planas įsigalioja įvykus elektroninės informacijos saugos incidentui, jo vykdymas yra privalomas elektroninės informacijos saugos incidentų atveju, kurių metu gali kilti pavojus informacinių sistemų duomenims, informacinių sistemų techninės, programinės įrangos funkcionavimui. Naudotojų veiksmai yra nurodyti Įstaigos Informacinių sistemų veiklos tęstinumo valdymo plane (Priedas Nr. 1).

4. Už Valdymo plano įgyvendinimo organizavimą ir įgyvendinimą atsakingi Įstaigos įgalioti darbuotojai.

5. Elektroninės informacijos saugos incidento metu patirti nuostoliai padengiami iš Įstaigos biudžeto ir kitų finansavimo šaltinių.

6. Kriterijai, pagal kuriuos nustatoma, kad informacinės sistemos veikla yra atkurta:

6.1. Informacinės sistemos duomenų atnaujinimas;

6.2. Informacinės sistemos duomenų išsaugojimas.

II SKYRIUS
ORGANIZACINĖS NUOSTATOS

7. Veiklos tęstinumo valdymo grupės sudėtis:

7.1. grupės vadovas – Įstaigos direktorius;

7.2. grupės vadovo pavaduotojas – Įstaigos direktoriaus pavaduotojas.

7.3. grupės nariai:

7.3.1. Ūkio ir aptarnavimo padalinio vadovas;

7.3.2. Finansų planavimo ir valdymo padalinio vadovas

7.3.3. Administratorius;

8. Veiklos tęstinumo valdymo grupės funkcijos:

8.1. analizuoti elektroninės informacijos saugos incidentus ir priimti sprendimus informacinės sistemos veiklos tęstinumo valdymo klausimais;

8.2. bendrauti su viešosios informacijos rengėjų ir viešosios informacijos skleidėjų atstovais;

8.3. bendrauti su kitų informacinių sistemų veiklos tęstinumo valdymo grupėmis;

8.4. bendrauti su teisėsaugos ir kitomis institucijomis, atsakingomis už nacionalinį elektroninių ryšių tinklų ir informacijos saugumą;

8.5. kontroliuoti finansinių ir kitų išteklių, reikalingų informacinės sistemos veiklai atkurti įvykus elektroninės informacijos saugos incidentui, naudojimą;

8.6. užtikrinti elektroninės informacijos fizinę saugą įvykus saugos incidentui;

8.7. organizuoti darbuotojų, daiktų, įrangos gabenimą;

8.8. vykdyti informacinių sistemų veiklos atkūrimo priežiūrą ir koordinuoti veiklos atkūrimo veiksmus;

8.9. vykdyti kitas Veiklos tęstinumo valdymo grupei pavestas funkcijas.

9. Veiklos atkūrimo grupės sudėtis:

9.1. grupės vadovas – Įstaigos direktorius;

9.2. grupės vadovo pavaduotojas – Įstaigos direktoriaus pavaduotojas;

9.3. grupės nariai:

9.3.1. Ūkio ir aptarnavimo padalinio vadovas

9.3.2. Finansų planavimo ir valdymo padalinio vadovas

9.3.3. Administratorius

10. Veiklos atkūrimo grupės funkcijos:

10.1. organizuoti informacinių sistemų tarnybinių stočių veikimo atkūrimą;

10.2. organizuoti kompiuterių tinklo veikimo atkūrimą;

10.3. organizuoti informacinių sistemų elektroninės informacijos atkūrimą;

10.4. organizuoti taikomųjų programų tinkamo veikimo atkūrimą;

10.5. organizuoti darbo kompiuterių veikimo atkūrimą ir prijungimą prie kompiuterių tinklo;

10.6. vykdyti kitas Veiklos atkūrimo grupei pavestas funkcijas.

11. Įvykus elektroninės informacijos saugos incidentui patalpose, kuriose yra saugoma informacinių sistemų techninė ir programinė įranga, įgaliotas darbuotojas:

11.1. nedelsdamas informuoja apie nenumatytą situaciją informacinės sistemos naudotojo vadovą ir informaciją įrašo į Elektroninės informacijos saugos incidentų registravimo žurnalą (Priedas Nr. 2), vadovauja veiklos tęstinumo plane nurodytiems veiksmams;

11.2. atkuria tarnybinės stoties, kompiuterių tinklo veiklą, duomenis, techninės, sisteminės ir taikomosios programinės įrangos funkcionavimą ir apie tai informuoja informacinės sistemos naudotojo vadovą;

11.3. organizuoja žalos informacinės sistemos duomenims, techninei bei programinei įrangai vertinimą, koordinuoja informacinės sistemos veiklai atkurti reikalingos techninės, sisteminės ir taikomosios programinės įrangos įsigijimą.

12. Įstaigos darbuotojų telefonų numeriai, jų elektroninio pašto adresai nuolat atnaujinami Įstaigos interneto svetainėje.

13. Elektroninės informacijos saugos incidento metu sunaikinta techninė, sisteminė ir taikomoji programinė įranga įsigyjama Viešųjų pirkimų įstatymo nustatyta tvarka, panaudojant Įstaigos biudžeto išteklius ar kitus finansavimo šaltinius.

III SKYRIUS
VEIKLOS ATKŪRIMO PRIORITETAI

14. Darbuotojų sveikatos ir gyvybės apsauga.
15. Informacinių technologijų veiklos atstatymas.
16. Kiek galima greitesnis sutrikusios Įstaigos veiklos atstatymas.

IV SKYRIUS
VEIKLOS TĘSTINUMO VALDYMAS

17. Visi Įstaigos darbuotojai turi būti supažindinti su jų pareigomis, sprendžiant kritines situacijas.

18. Įvykus kritinei situacijai ar iškilus grėsmei, pirmiausiai apie tai informuojamas Įstaigos vadovas ar jį pavaduojantis asmuo bei Veiklos atkūrimo komanda.

19. Veiklos atkūrimo komanda, įvertinusi kritinės situacijos mastą ir nustačius, kad Įstaigos veikla gali būti sutrikdyta ilgiau nei 1 (vienai) dienai, inicijuoja kritinės situacijos valdymo veiksmus, padarinių šalinimui.

20. Veiklos atkūrimo komanda organizuoja žalos techninei, programinei įrangai vertinimą, koordinuoja techninės, sisteminės ir taikomosios programinės įrangos Įstaigos veiklai atkurti įsigijimą.

21. Ne rečiau kaip kartą per metus Veiklos atkūrimo komanda inicijuoja veiklos tęstinumo valdymo testavimą ir nustato testavimo apimtį, parenkant vieną, kelis ar visus scenarijus.

22. Plano testavimai atliekami vienu iš pasirinktu metodu: teorinio modeliavimo metodu, dalinio testavimo metodu arba kritinės situacijos imitavimo metodu.

23. Testavimo rezultatai dokumentuojami.

24. Plano veiksmingumo išbandymo metu pastebėti trūkumai šalinami remiantis operatyvumo, veiksmingumo ir ekonomiškumo principais.

Priedas Nr. 1
Informacinių sistemų veiklos tęstinumo valdymo planas

Pavojaus rūšys	Pirmaeiliai veiksmai	Pasekmių likvidavimo veiksmai	Pasekmių likvidavimo atsakingi vykdytojai
1. Oro sąlygos	1.1. Elektroninės informacijos saugos incidento pasekmės įvertinimas, priemonių plano pavojui sustabdyti ir padarytai žalai likviduoti sudarymas ir įgyvendinimas	1.1.1. Elektroninės informacijos saugos incidento metu padarytos žalos įvertinimas	Veiklos atkūrimo grupė
		1.1.2. Pavojaus sustabdymo ir padarytos žalos likvidavimo priemonių plano sudarymas ir paskelbimas	Veiklos tęstinumo valdymo grupė
		1.1.3. Priemonių plano įgyvendinimas	Veiklos atkūrimo grupė
	1.2. Darbuotojų elektroninės informacijos saugos incidento pasekmei likviduoti paskyrimas	1.2.1. Žalą likviduojančių darbuotojų apmokymas	Veiklos atkūrimo grupė
		1.2.2. Žalą likviduojančių darbuotojų veiksmų koordinavimas	Veiklos tęstinumo valdymo grupė
	1.3. Oro prognozės sekimas	1.3.1. Žalą likviduojančių darbuotojų instruktavimas	Veiklos atkūrimo grupė
	1.4. Dirbantiesiems pavojaus vietoje rekomendacijų teikimas	1.4.1. Elektroninės informacijos saugos incidento pasekmes likviduojančių darbuotojų apmokymas	Veiklos atkūrimo grupė
		1.4.2. Darbuotojų informavimas apie elgseną pavojaus vietoje	Veiklos tęstinumo valdymo grupė
		1.4.3. Pirmosios pagalbos suteikimo organizavimas nukentėjusiems darbuotojams	Veiklos tęstinumo valdymo grupė
		1.4.4. Nukentėjusių darbuotojų gabenimo į gydymo įstaigą organizavimas	Veiklos tęstinumo valdymo grupė
	1.5. Pavojaus vietų ženklinimas	1.5.1. Darbuotojų informavimas	Veiklos tęstinumo valdymo grupė
		1.5.2. Žalą likviduojančių darbuotojų apmokymas	Įgaliotas darbuotojas
2. Gaisras	2.1. Ugniagesių tarnybos informavimas	2.1.1. Įvykio vietos lokalizavimas, jei gauta rekomendacija	Veiklos tęstinumo valdymo grupė

Pavojaus rūšys	Pirmaeiliai veiksmai	Pasekmių likvidavimo veiksmai	Pasekmių likvidavimo atsakingi vykdytojai
		2.1.2. Galimybių evakuoti darbuotojus paieška, jei yra rekomenduojama tai padaryti	Veiklos tęstinumo valdymo grupė
	2.2. Darbuotojų evakavimas (pagal ugniagesių tarnybos rekomendaciją)	2.2.1. Darbuotojų informavimas apie evakavimą, jei yra rekomendacija	Veiklos tęstinumo valdymo grupė
	2.3. Darbas pavojaus zonoje	2.3.1. Darbuotojų informavimas apie saugų darbą pavojaus zonoje	Veiklos tęstinumo valdymo grupė
	2.4. Komunikacijų, sukeliančių pavojų, išjungimas. Gaisro gesinimas ankstyvoje stadijoje, jei yra rekomendacija dirbti pavojaus zonoje	2.4.1. Ugniagesių tarnybos nurodymų vykdymas	Veiklos atkūrimo grupė
3. Patalpų užgrobimas	3.1.Teisėsaugos tarnybos informavimas	3.1.1. Įvykio vietos lokalizavimas, jei yra teisėsaugos tarnybos rekomendacijos	Veiklos tęstinumo valdymo grupė
		3.1.2. Galimybių evakuoti darbuotojus nagrinėjimas, jei gauta rekomendacija	Veiklos tęstinumo valdymo grupė
	3.2. Darbuotojų evakavimas, jei yra rekomendacija	3.2.1. Darbuotojų informavimas apie evakavimą	Veiklos tęstinumo valdymo grupė
	3.3. Patalpų užrakinimas, jei yra galimybė	3.3.1. Teisėsaugos tarnybos nurodymų vykdymas	IS naudotojų padalinio vadovas
	3.4. Teisėsaugos tarnybos nurodymų vykdymas, jei yra rekomendacija	3.4.1. Darbuotojų informavimas apie nurodymų vykdymą	Veiklos tęstinumo valdymo grupė
	3.5. Veiksmai išlaisvinus užgrobtas patalpas	3.5.1. Padarytos žalos įvertinimas	Veiklos atkūrimo grupė
		3.5.2. Padarytos žalos likvidavimo priemonių plano sudarymas, paskelbimas, vykdymas	Veiklos atkūrimo grupė
		3.5.3. Žalą likviduojančių darbuotojų apmokymas	Veiklos atkūrimo grupė
4. Patalpai padaryta žala		4.1.1. Rekomendacijų iš suinteresuotos tarnybos gavimas apie galimybę dirbti pavojaus zonoje	Veiklos tęstinumo valdymo grupė

Pavojaus rūšys	Pirmaeiliai veiksmai	Pasekmių likvidavimo veiksmai	Pasekmių likvidavimo atsakingi vykdytojai
arba patalpos praradimas	4.1. Atitinkamos tarnybos informavimas apie pavojaus pobūdį	4.1.2. Darbuotojų informavimas apie rekomendacijas	Veiklos tęstinumo valdymo grupė
	4.2. Atsarginių patalpų įrengimas	4.2.1. Darbuotojų informavimas apie darbą patalpose	Veiklos tęstinumo valdymo grupė
5. Energijos tiekimo sutrikimai	5.1. Energijos tiekimo sutrikimo priežasčių nustatymas. Tarnybinės stoties, kitos techninės įrangos energijos maitinimo išjungimas	5.1.1. Sutrikimų šalinimo organizavimas	Veiklos tęstinumo valdymo grupė
	5.2. Kreipimasis į energijos tiekimo tarnybą dėl pavojaus trukmės ir sutrikimo pašalinimo galimybių	5.2.1. Rekomendacijų iš energijos tiekimo tarnybos gavimas	Veiklos tęstinumo valdymo grupė
	5.3. Sutrikimų pašalinimas	5.3.1. Pavojaus sustabdymas, padarytos žalos likvidavimo priemonių plano sudarymas ir įgyvendinimas	Veiklos atkūrimo grupė
		5.3.2. Padarytos žalos įvertinimas	
		5.3.3. Žalą likviduojančių darbuotojų apmokymas	Veiklos atkūrimo grupė
6. Vandentiekio ir šildymo sistemos sutrikimai	6.1. Vandentiekio ar šildymo paslaugų teikėjų informavimas	6.1.1. Atitinkamos tarnybos paklausimas dėl leidimo dirbti ir rekomendacijų gavimas	Veiklos tęstinumo valdymo grupė
		6.1.2. Darbuotojų informavimas apie rekomendacijas	Veiklos tęstinumo valdymo grupė
	6.2. Sutrikimo šalinimo prognozės skelbimas, sutrikimo pašalinimas	6.2.1. Padarytos žalos įvertinimas. Sutrikimo sustabdymo ir padarytos žalos likvidavimo priemonių plano sudarymas, plano įgyvendinimas	Veiklos atkūrimo grupė
		6.2.2. Žalą likviduojančių darbuotojų apmokymas	Veiklos atkūrimo grupė
7. Ryšio sutrikimai	7.1. Ryšio sutrikimo priežasčių nustatymas	7.1.1. Kreiptis į ryšio paslaugos teikėją	Veiklos tęstinumo valdymo grupė

Pavojaus rūšys	Pirmaeiliai veiksmai	Pasekmių likvidavimo veiksmai	Pasekmių likvidavimo atsakingi vykdytojai
	7.2. Ryšio tarnybų informavimas, paklausimo dėl sutrikimo trukmės ir pašalinimo prognozės	7.1.2. Nustatyti ir įgyvendinti priemones, kad sutrikimai nesikartotų	
	7.3. Sutrikimo pašalinimas	7.1.3. Kreiptis į kitą ryšio paslaugos teikėją, jei sutrikimas nepašalintas	Veiklos tęstinumo valdymo grupė
8. Tarnybinės stoties, komutacinės įrangos sugadinimas	8.1. Pranešti teisėsaugos tarnybai, draudimo bendrovei apie įvykį	8.1.1. Darbuotojų elektroninės informacijos saugos incidento pasekmei likviduoti paskyrimas, apmokymas, jų veiksmų nustatymas	Veiklos tęstinumo valdymo grupė
	8.2. Elektroninės informacijos saugos incidento pasekmių šalinimas	8.2.1. Kreiptis į įrangos tiekėjus dėl įrangos remonto ar naujos įrangos įsigijimo	Veiklos atkūrimo grupė
		8.2.2. Įsigytos įrangos diegimas	Veiklos atkūrimo grupė
9. Programinės įrangos sugadinimas, praradimas	9.1. Elektroninės informacijos saugos incidento pasekmių įvertinimas, priemonių plano pavojui sustabdyti ir padarytai žalai likviduoti sudarymas	9.1.1. Elektroninės informacijos saugos incidento metu padarytos žalos įvertinimas	Veiklos atkūrimo grupė
		9.1.2. Priemonių plano sudarymas, paskelbimas ir įgyvendinimas	Veiklos tęstinumo valdymo grupė
	9.2. Darbuotojų elektroninės informacijos saugos incidento pasekmėms likviduoti paskyrimas. Žalą likviduojančių darbuotojų instruktavimas, jų veiksmų koordinavimas	9.2.1. Žalą likviduojančių darbuotojų apmokymas	
		9.2.2. Kreipimasis į teisėsaugos tarnybas dėl programinės įrangos sugadinimo ar praradimo ir jų nurodymų vykdymas	Veiklos tęstinumo valdymo grupė
10. Dokumentų praradimas	10.1. Elektroninės informacijos saugos incidento pasekmių įvertinimas	10.1.1. Prarastų dokumentų atkūrimas	Veiklos atkūrimo grupė
		10.1.2. Prarastų dokumentų atkūrimo kontrolė	Veiklos tęstinumo valdymo grupė
11. Darbuotojų praradimas	11.1. Elektroninės informacijos saugos incidento pasekmių įvertinimas	11.1.1. Trūkstamų darbuotojų paieška ir priėmimas į darbą	Veiklos tęstinumo valdymo grupė

Priedas Nr. 2
Elektroninės informacijos saugos incidentų registravimo žurnalas

Eil. Nr.	Elektroninės informacijos saugos incidentas						
	IS naudotojo padalinio pavadinimas	**Požymio kodas***	**Įvykio aprašymas**	**Pradžia (metai, mėnuo, diena, valanda)**	**Pabaiga (metai, mėnuo, diena, valanda)**	**Pašalino (vardas, pavardė)**	**Įgaliotas darbuotojas (vardas, pavardė, parašas)**
1.							
2.							
3.							
4.							
5.							
6.							

* Elektroninės informacijos saugos incidento situacijos požymiai:
1. Oro sąlygos. 2. Gaisras. 3. Patalpų užgrobimas. 4. Patalpai padaryta žala arba patalpos praradimas. 5. Energijos tiekimo sutrikimai.
6. Vandentiekio ir šildymo sistemos sutrikimai; 7. Ryšio sutrikimai. 8. Tarnybinės stoties, komutacinės įrangos sugadinimas, praradimas.
9. Programinės įrangos sugadinimas, praradimas. 10. Duomenų pakeitimas, sunaikinimas, atskleidimas, dokumentų praradimas.
11. Darbuotojų praradimas.