

DRUSKININKŲ SPORTO CENTRO INFORMACIJOS APDOROJIMO PRIEMONIŲ NAUDOJIMO TVARKOS APRAŠAS

I SKYRIUS BENDROSIOS NUOSTATOS

1. Druskininkų sporto centro (toliau – Centras) informacijos apdorojimo priemonių naudojimo tvarkos aprašas (toliau – Aprašas) nustato Centro kompiuterių ir programinės įrangos diegimą, eksploatavimą, apskaitą ir apibrėžia teisėtą, saugaus ir etiško Centro kompiuterių, tinklo ir interneto išteklių naudojimo principus visiems asmenims, dirbantiems Centre.

II SKYRIUS PAGRINDINĖS SĄVOKOS

2. **Administratorius** – tiekėjas, su kuriuo sudaryta paslaugų teikimo sutartis ir kuriam suteikta teisė tvarkyti Centro kompiuterinę įrangą, diegti pagrindinę įrangą, prižiūrėti kompiuterių tinklą ir kompiuterines sistemas.

3. **Duomenų šifravimas** – duomenų formos pakeitimas iš paprastos į specifinę, iš kurios duomenis galima pakeisti į pradinę formą tik žinant duomenų pakeitimo algoritmą.

4. **Kompiuterinė įranga** – tai sisteminis blokas ar nešiojamas kompiuteris ir jo dalys, išoriniai įrenginiai (monitoriai, skaitytuvai, spausdintuvai bei kopijavimo aparatai, klaviatūros, pelės, kolonėlės, ausinės, vaizdo bei fotokameros, multimedijos projektoriai ir pan.), kompiuterių tinklo įranga, kompiuterių bei tinklo įrangos montavimo spintos, nuolatinio elektros maitinimo šaltiniai ir kt.

5. **Kompiuterio naudotojas** – Darbuotojas, dirbantis kompiuterine ir/ar programine įranga.

6. **Kompiuterių tinklas** – tai serveriai ir darbo vietų kompiuteriai, kompiuterių tinklo įranga (kabeliai, tinklo aparatūra) sujungti į vieningą sistemą, siekiant užtikrinti kompiuterių naudotojams operatyvų keitimąsi informacija, kolektyvinį kompiuterių ir programinės įrangos bei interneto paslaugų naudojimą.

7. **Programinė įranga** – tai kompiuterių programos, skirtos kompiuterių įrangos valdymui bei kompiuterio naudotojo uždavinių sprendimui kompiuteriu (operacinės sistemos, programavimo sistemos, biuro programų paketai, antivirusinės, archyvavimo bei kitos taikomosios programos).

8. **Privilegiuota prieiga** – teisių rinkinys, suteikiantis teisę Darbuotojui administruoti informacines sistemas techniniu ir programiniu lygmeniu ir atlikti kitas Administratoriaus teisių reikalaujančias funkcijas ar atlikti informacijos saugos įgaliojimo funkcijas.

9. **Keitimas** – bet kurios informacijos apdorojimo priemonės arba jos elemento pridėjimas, išėmimas iš arba modifikavimas.

10. **Keitimų valdymas** – procesas keitimų gyvavimo ciklui valdyti, kurios pagrindinis tikslas – leisti atlikti naudingus pokyčius minimaliai trikhdant Centro veiklą. Keitimai turi būti lengvai atsekami ir išsamiai dokumentuojami.

11. **Kompiuterių tinklo naudotojas** – tai kompiuterio tinklo naudotojams prieinamos interneto paslaugos (www, elektroninis paštas ir pan.), kompiuterių naudotojams skirta atmintis serverių diskuose, kolektyviai naudojama programinė įranga ir panašiai.

12. **IS** – Informacinė sistema.
13. **IT** – Informacinės technologijos.
14. **Incidentas** – realų ar potencialiai nepageidaujamą poveikį kompiuterio ar kompiuterių tinklo veiklai turintis įvykis, kurio rezultatas – apgaulė, įsilaužimas į tinklo kompiuterius, kompiuterinių virusų arba nepageidaujamų laiškų atakos nuostoliai ar piktnaudžiavimas, grėsmė informacijai, informacijos nuosavybės praradimas ar žala jai, kiti kompiuterių tinklą trikdančios veiksmas.
15. **Informacija** – visi kompiuteryje saugomi duomenų rinkiniai.
16. Informacijos apdorojimo priemonės – kompiuterių techninė ir programinė įranga.
17. **Materialiai atsakingas darbuotojas** – Centro darbuotojas, atsakingas už informacijos valdymą.
18. **Failų serveris** – duomenų laikymo įrenginys, prijungtas prie Centro kompiuterių tinklo ir pasiekiamas visiems to tinklo naudotojams. Į failų serverį vienu metu gali kreiptis keli naudotojai.
19. **Patikrinimas** – procedūra, kurios metu susipažįstama su Darbuotojo elektroninio pašto turiniu, laikantis Apraše nustatytos tvarkos.

III KYRIUS KOMPIUTERIO NAUDOJIMAS

20. Darbuotojui jo darbo Centre laikotarpiu skiriamas kompiuteris jo darbo funkcijoms vykdyti.
21. Kompiuteryje įdiegta ir periodiškai atnaujinama antivirusinė Programinė įranga.
22. Programinės įrangos diegimą, konfigūravimą ir šalinimą atlieka Administratorius.
23. Programinės įrangos diegimo, konfigūravimo ir šalinimo paslaugų organizavimą ir kontrolę atlieka Centro ūkvedys.
24. Kompiuterinės įrangos naudotojui draudžiama:
 - 24.1. leisti naudotis Kompiuterine įranga pašaliniam asmeniui;
 - 24.2. taisyti, laužyti ir gadinti Kompiuterinę įrangą, kitą išduotą Centro IT turtą;
 - 24.3. savavališkai keisti jam priskirtą Kompiuterinę įrangą (pakeisti kompiuterį, spausdintuvą, monitorių, klaviatūrą, pelę ir pan.), taip pat savarankiškai perkelti sumontuotą Kompiuterinę įrangą į kitą vietą. Visus techninių priemonių perkėlimas darbo vietoje bei tarp Kompiuterių tinklo naudotojų organizuoja Centro ūkvedys;
 - 24.4. išnešti iš Centro patalpų Kompiuterinę įrangą išskyrus naudojantiems nešiojamuosius kompiuterius ar kitą Kompiuterinę įrangą, kai tai būtina tiesioginėms darbo funkcijoms vykdyti. Šis draudimas netaikomas, vykdant Kompiuterinės įrangos taisymo ir priežiūros funkcijas, kurias organizuoja Centro ūkvedys;
 - 24.5. naudoti Kompiuterinę įrangą veiklai, kuri nesuderinama su darbuotojo atliekamomis funkcijomis, etika;
 - 24.6. atlikti veiksmus, pažeidžiančius fizinio ar juridinio asmens teises, kurias saugo autorių, gretutinių ir intelektualios nuosavybės (pvz.: dainos, filmai ir kt.) teisių apsaugos įstatymai. Tarp tokių veiksmų yra savavališkas Programinės įrangos diegimas, naudojimas, saugojimas arba platinimas, neturint licencijos, neleistas autorių teisėmis apsaugotų kūrinių kopijavimas;
 - 24.7. vykdyti ar atidarinti piktybines programas (t. y. kompiuterinius virusus „Trojaus arklius“ ir pan.);
 - 24.8. atskleisti prisijungimo duomenis prie kompiuterio, Centro naudojamų sistemų ir informacijos išteklių prisijungimo vardus, slaptažodžius arba leisti naudotis savo prisijungimo duomenis kitiems asmenims;
 - 24.9. naudoti programas ir atlikti bet kokio pobūdžio veiksmus, kurie sunkina ar trikdo kompiuterio veikimą arba gali sukelti incidentą kompiuterių tinkluose;
 - 24.10. savavališkai keisti suteiktus kompiuterio tinklo parametrus (IP adresą ir ap.);

24.11. savavališkai trinti, manipuliuoti ir iškreipti darbo metu gautą, naudojamą bei sukurtą informaciją siekiant pakenkti Centrai ar jo darbuotojams;

24.12. naršyti pornografiniuose, smurta, terorizmą bei kitokią nusikalstamą veiklą programuojančiuose tinklapiuose, elektroniniu paštu platinti elektronines šiukšles, piktybines programas, virusus, įsilaužti į kitas kompiuterines sistemas;

24.13. vykdyti failų mainus tarp interneto vartotojų naudojant lygiavertiškumo (angl. Peer topeer, P2P) tipo programas (pvz.: „uTorrent“, „eMule“, „DC++“, „BitComet“ ir kt.);

24.14. įdiegti ir pašalinti taikomąsias ar kitokio pobūdžio programas, išskyrus, kai tai daro Administratorius;

24.15. nesankcionuotai naudotis svetimais kompiuterių ir kitais informacinių technologijų ištekliais (kopijuoti ir naudotis programomis ir duomenimis be išteklių savininko žinios ir sutikimo, jungtis prie svetimų kompiuterių be atitinkamo leidimo ir pan.), išskyrus Administratoriui, kuris turi tokią teisę. Centro darbo tikslais, užtikrinant konfidencialios informacijos apsaugą ir kitus informacijos saugos aspektus;

24.16. atlikti bet kokius kitus veiksmus, pažeidžiančius ES ir nacionalinės teisės aktus;

25. Kompiuterio naudotojas privalo:

25.1. įvykus incidentui ar kilus klausimams dėl kompiuterio naudojimo kreiptis/informuoti Centro ūkvedį raštu;

25.2. leisti Administratoriui įvertinti kompiuterio būklę;

25.3. naudoti jam skirtą Kompiuterinę įrangą efektyviai ir pagal paskirtį, taupyti išteklius;

25.4. baigus darbą, uždaryti visas programas, išsiregistruoti iš savo Kompiuterio naudotojo aplinkos ir išjungti kompiuterį.

IV SKYRIUS

NEŠIOJAMŲ KOMPIUTERIŲ IR MOBILIŲJŲ ĮRENGINIŲ NAUDOJIMAS

26. Nešiojamų kompiuterių ir mobiliųjų įrenginių naudojimui (toliau – Nešiojami įrenginiai), įskaitant asmeninius įrenginius, naudojamus darbui, taikomi Aprašo IV dalyje nurodyti naudojimosi reikalavimai ir žemiau nurodytos papildomos apsaugos priemonės:

26.1. Centro ūkvedys kartą per metus privalo organizuoti Nešiojamų įrenginių patikrą ir priežiūrą. Patikrą galima atlikti nuotoliniu būdu, prisijungus prie Nešiojamo įrenginio (kai Nešiojamas įrenginys prijungtas prie vidinio kompiuterių tinklo), naudojant Nešiojamų įrenginių valdymo sistemą arba darbuotojui fiziškai pristčius Nešiojamą įrenginį;

26.2. Darbuotojai jiems Centro suteiktus Nešiojamus įrenginius privalo naudoti tik Centro darbo funkcijoms vykdyti;

26.3. Darbuotojai privalo laikytis šių Nešiojamų įrenginių naudojimo reikalavimų:

26.3.1. saugoti Nešiojamą įrenginį nuo aplinkos poveikio – dulkių, vibracijos, cheminių medžiagų, elektromagnetinio spinduliavimo;

26.3.2. saugoti nuo didelių temperatūros pokyčių;

26.3.3. nepalikti Nešiojamo įrenginio be priežiūros viešose vietose;

26.3.4. kelionių metu registruoti Nešiojamą įrenginį kaip rankinį bagažą;

26.3.5. nesinaudojant mobiliuoju įrenginiu, apsaugoti jį slaptažodžiu arba biometrinėmis apsaugos priemonėmis;

26.3.6. nenaudojamus Nešiojamus įrenginius grąžinti atsakingam Centro darbuotojui;

26.3.7. pametus Nešiojamą įrenginį ar įvykus jo vagystei, nedelsiant informuoti administratorių.

27. Darbuotojams draudžiama:

27.1. mėtyti, laužyti, daužyti, ardyti Nešiojamus įrenginius, dėti ant jų sunkius daiktus;

27.2. bandyti šalinti, apeiti ar išjungti įrenginyje nustatytas saugumo priemones;

27.3. leisti naudotis nešiojamu įrenginiu kitiems žmonėms;

27.4. išimti Nešiojamo įrenginio bateriją jo neišjungus ar kitaip pažeisti gamintojo nustatytas eksploataavimo rekomendacijas.

V SKYRIUS SLAPTAŽODŽIŲ NAUDOJIMAS

28. Darbuotojai privalo saugoti slaptažodžius, neatskleisti jų kitiems asmenims, nelaikyti matomose ir lengvai kitiems asmenims prieinamose vietose ir laikytis šių reikalavimų:

28.1. leistinas prisijungimų prie savo kompiuterinės darbo aplinkos (paskyros) bandymų skaičius – 5. Po 5 nesėkmingų bandymų prisijungti prie savo kompiuterinės darbo aplinkos (paskyros) paskyra blokuojama, paskyros valdytojas privalo kreiptis į Centro ūkvedį;

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

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. slaptažodį naudotojui galima keisti antrą kartą ne anksčiau kaip po 1 dienos;

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

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

VI SKYRIUS PRIEIGOS VALDYMAS

29. Darbuotojams prieiga prie informacinių išteklių suteikiama Darbuotojo pareigų ir vaidmenų Centro veiklos procesuose pagrindu.

30. Darbuotojams suteikiama tiek prieigos teisių, kiek jiems būtina atlikti darbo funkcijoms.

31. Darbuotojo ir Administratoriaus prieigos teisės yra atskirtos, naudojant skirtingas paskyras.

32. Privilegijuotos prieigos teisių nenaudoti įprastai veiklai, kurią galima vykdyti turint Darbuotojo prieigos teises, atlikti. Privilegijuotos prieigos teisės negali apimti prieigos prie konfidencialios informacijos arba padidinto konfidencialumo informacijos, išskyrus atvejus, kai to reikia jų įprastai IT pagalbos veiklai atlikti.

33. Privilegijuotos prieigos teisės paskiriamos Centro direktoriaus įsakymu.

34. Prieiga prie Centro informacinių išteklių suteikiama Darbuotojo tiesioginio vadovo prašymu. Informaciją apie reikalingas suteikti prieigas asmeniui, Administratorius gauna tiesiogiai iš priimamo Darbuotojo tiesioginio vadovo po to, kai Centro direktorius pasirašo įsakymą dėl prieigos suteikimo.

35. Kai keičiasi Darbuotojo pareigos ar vaidmenys Centre arba Darbuotojas atleidžiamas iš darbo, tiesioginis Darbuotojo vadovas nedelsiant elektroniniu paštu informuoja apie tai Administratorių, kuris atsakingas už prieigos suteikimą.

36. Prieigos teisės turi būti suteikiamos, vadovaujantis tiesioginio Darbuotojo vadovo pavedimu pagal jame nurodytas Darbuotojo pareigas ir vaidmenį.

37. Trečiosioms šalims prieiga prie Centro informacinių išteklių suteikiama sutartyse su trečiosiomis šalimis nustatyta tvarka ir tik pasirašius konfidencialumo susitarimus.

38. Visi prieigų teisių turėtojų registravimo ar šios informacijos pakeitimai turi būti išsaugomi IS priežiūros žurnale.

39. Periodiškai, ne rečiau kaip kartą per metus, organizuoja naudotojų prieigos teisių turėtojų ir slaptažodžių naudojimo reikalavimų laikymosi peržiūrą.

VII SKYRIUS NEŠIOJAMŲ LAIKMENŲ NAUDOJIMAS

40. Darbuotojams draudžiama jungti ne Centro duomenų laikmenas (CD ir DVD įrenginius, išorinius kietuosius diskus, USB atminties korteles) prie Centro kompiuterių, išskyrus Centro išduotas ir Administratoriaus patikrintas laikmenas. Esant darbiniam poreikiui, ne Centro išduotą duomenų laikmeną galima įjungti į Centro Kompiuterinę įrangą, prieš tai patikrinus Administratoriui.

41. Nešiojamose duomenų laikmenose saugoma padidinto konfidencialumo, konfidenciali informacija, asmenų, susijusių darbo santykiais būti šifruojami.

42. Nenaudojamas arba sugedusias keičiamas duomenų laikmenas Darbuotojai turi gražinti Centro ūkvedžiui, kuris yra atsakingas už saugų laikmenose esančios informacijos sunaikinimą.

43. Darbuotojai turi užtikrinti, kad perdavimo metu duomenų laikmenos su įrašyta informacija patektų nurodytam informacijos gavėjui ir būtų apsaugotos nuo neteisėtos prieigos ar sugadinimo.

44. Nesant galimybei duomenų laikmenų perduoti asmeniškai informacijos gavėjui, turi būti naudojami patikimi siuntų vežėjai, užtikrinantys duomenų laikmenos pristatymą nurodytam gavėjui.

VIII SKYRIUS KOMPIUTERIŲ TINKLO NAUDOJIMAS

45. Galimybė naudotis Centro kompiuterių tinklu ir Kompiuterių tinklo ištekliais suteikiama tik darbo Centre laikotarpiu.

46. Centro kompiuterių tinklo ištekliai skirti profesiniam darbui, kvalifikacijos kėlimui. Asmeniniais tikslais kompiuterių tinklo ištekliais Darbuotojai gali naudotis tiek, kiek tai netrukdo jam atlikti pareigas Centre ir neprieštaruoja etiško elgesio normoms.

47. Bevielio tinklo prieigai (WI-FI) Centro patalpose yra sukonfigūruotos stotelės, kurios skirtos Darbuotojams ir Centro svečiams. Bevielio tinklo slaptažodžius suteikia ir keičia Centro ūkvedys.

48. Informacijos saugumo užtikrinimui Centro svečiams suteikiamas tik (svečiams skirtas) prisijungimo prie bevielio tinklo slaptažodis.

49. Darbuotojai atsako už veiksmus, kurie kenkia kompiuterinei, kompiuterių tinklo įrangai ir informacijai, atliktus pasinaudojus disponuojamais ištekliais arba atliktus jo vardu.

50. Kompiuterių tinkle draudžiama:

50.1. leisti naudotis Centro kompiuterių tinklo ištekliais ir teikiamomis paslaugomis juridiniams ir fiziniams asmenims, kurie tiesiogiai nesusiję su Centru ar jos veikla;

50.2. naudoti tinklo išteklius tarptautinėje teisėje ir praktikoje pripažinti neteisėtai veiklai vykdyti, taip pat Lietuvos Respublikos įstatymų ir kitų teisės aktų draudžiamai veiklai;

50.3. kompiuterio tinklo išteklius naudoti komercinei veiklai, smurto, amoralaus elgesio skatinimui, komentarų rašymui, įžeidžiančių dalykų skleidimui ir pan.;

50.4. žiūrėti, kausti arba platinti pornografinę, rasinę, tautinę neapykantą ar smurtą propaguojančią medžiagą, Įstaigos vardą diskredituojančią medžiagą, kitus juridinius ir fizinius asmenis ar valstybę įžeidžiančią informaciją;

50.5. dalyvauti lažybose ir azartiniuose lošimuose internetu, žaisti internetinius žaidimus;

50.6. įžeidžiančiai ar kitaip žmonių moralę žeminančiai komentuoti interneto svetainėse;

50.7. užsiimti veikla, kuri nesuderinama su Darbuotojo etika;

50.8. parsisiųsti arba platinti Programinę įrangą arba kitą informaciją, kurios diegimas, naudojimas arba platinimas prieštarautų Lietuvos Respublikos autorių teisių ir gretutinių teisių įstatymo, Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymo reikalavimams arba Komisijos teisės aktų nuostatom;

50.9. skelbti Centro Kompiuterių tinklo ištekliuose su Centro veikla nesusijusius ir asmeninius tinklalapius;

50.10. savavališkai keisti Kompiuterių tinklo išteklių parametrus, susijusius su apsauga, arba prisijungiant apeiti bet kurį iš įdiegtų saugumo mechanizmų;

50.11. darbo vietos kompiuteryje blokuoti antivirusines priemones;

50.12. atskleisti bevielio tinklo prisijungimo duomenis tretiesiems asmenims;

50.13. instaliuoti programas bei savavališkai šalinti svetimas bylas, kopijuoti, laikyti ir žaisti žaidimus;

50.14. perduoti Kompiuterio tinklo naudotojui suteiktas teises bei išteklius ar teikti kompiuterių tinklo paslaugas tretiesiems asmenims;

50.15. naudotis neskirtais ištekliais, kopijuoti įdiegtas programas, kitais būdais pažeidinėti saugumą, privatumą, tvarką ir kitų kompiuterių naudotojų teises;

50.16. skleisti melagingą informaciją, įžeidinėti ar priekabauti prie kitų asmenų naudojant Centro kompiuterių tinklo sistemas arba siųsti tokią informaciją, pasinaudojant Centro vardu;

50.17. naudoti programas ar atlikti bet kokio pobūdžio veiksmus, kurie sunkina ar trikdo tinklo veikimą arba gali sukelti incidentą kompiuteriuose ar kompiuterių tinkle (neautorizuotas servisų naudojimas, konfidencialios informacijos atskleidimas ar pakeitimas, servisų darbo sutrikdymas, kompiuterių virusai, tinklo skenavimo programos, tinklo blokavimo programos ir kt.);

50.18. pasirašyti apsimetus kitu asmeniu, ar įstaiga;

50.19. be išankstinės Centro ūkvedžio arba vadovų žinios naudoti asmeninę Kompiuterinę ir Programinę įrangą, jungti ją į Centro tinklą.

51. Kompiuterių tinklo naudotojas privalo:

51.1. laikytis etikos normų ir atsakyti už informaciją, pateiktą į kompiuterių tinklus;

51.2. laikytis Centro ūkvedžio ar Administratoriaus nurodymų, vykdyti visus nurodymus, susijusius su kompiuterių tinklo valdymu bei saugumu;

51.3. įvykus kompiuteriniam incidentui, nedelsiant informuoti Centro ūkvedį raštu;

51.4. saugoti jam suteiktus prisijungimo vardus ir slaptažodžius;

51.5. naudoti jam skirtus Kompiuterių tinklo išteklius pagal paskirtį.

52. Kompiuterių tinklo naudotojo teisės:

52.1. blokuoti savo informaciją nuo kitų Kompiuterių tinklo naudotojų neleistino naudojimosi;

52.2. iškilus problemų dėl kompiuterių tinklo veikimo, kreiptis į Centro ūkvedį raštu;

52.3. naudotis bendra vieta Failų serveryje, elektroniniu paštu, interneto tinklu ar kita informacine sistema, vykdant darbo funkcijas.

IX SKYRIUS

LICENCIJUOTOS PROGRAMINĖS ĮRANGOS NAUDOJIMAS

53. Naudojama tik licencijuota ir legali Programinė įranga.
54. Programinę įrangą galima naudoti tik jos licencijoje nurodyta tvarka.
55. Programinė įranga negali būti perduota kitam Kompiuterių tinklo naudotojui be Centro ūkvedžio ar Administratoriaus žinios.
56. Licencijuotos Programinės įrangos naudojimo tvarkos laikymąsi užtikrina kiekvienas Kompiuterių tinklo naudotojas.
57. Už Programinės įrangos naudojimą be licencijų Kompiuterių tinklo naudotojai atsako įstatymų nustatyta tvarka.

X SKYRIUS

VEIKLA CENTRO INTERNETO SVETAINĖJE

58. Centro interneto svetainė administruojama, vadovaujantis Bendrųjų reikalavimų valstybės ir savivaldybėms institucijų interneto svetainėms aprašu, patvirtintu Lietuvos Respublikos Vyriausybės 2003 m. balandžio 18 d. nutarimu Nr. 480 „Dėl bendrųjų reikalavimų valstybės ir savivaldybių institucijų ir įstaigų interneto svetainėms aprašo patvirtinimo“.
59. Už Centro svetainės tinkamą ir teisėtą funkcionavimą yra atsakingas Centro vadybininkas.
60. Už į Centro interneto svetainėje savalaikį informacijos talpinimą atsakingas Darbuotojas, kurio kompetencijai priklauso atitinkamos informacijos rengimas.

XI SKYRIUS

AUTOMATINIAI KOMPIUTERIO OPERACINĖS SISTEMOS ATNAUJINIMAI

61. Sėkmingam ir saugiam darbo vietų kompiuterių ir tarnybinių stočių darbui užtikrinti reikalinga, kad įrenginių operacinės sistemos būtų nuolat atnaujinamos. Šiam tikslui virtualiame serveryje *MultiSRV* įdiegta *WSUS (Windows Server Update Services)* tarnyba, kuri gauna aktualius atnaujinimus iš gamintojo portalo ir užtikrina jų pristatymą darbo vietų ir tarnybinių stočių kompiuteriams.
62. Kompiuteriui 11 val. automatiškai per *WSUS* diegiami atnaujinimai (dažniausiai kartą per savaitę). Įdiegus atnaujinimus gali reikėti kompiuterį paleisti iš naujo. Jeigu kompiuterio naudotojas į pasirodžiusį pranešimą/lentelę nereaguoja ir nepakeičia kompiuterio paleidimo iš naujo laiko į ilgesnį laiką nei standartinis – 10 min., tai kompiuteris bus paleistas iš naujo automatiškai praėjus konkrečiam laiko tarpui.
63. Rekomenduojama išsaugoti dokumentus prieš pasitraukiant nuo kompiuterio, nes kompiuteris gali būti paleistas iš naujo be kompiuterio naudotojo žinios, jeigu kompiuterio paleidimo iš naujo atidėjimo nustatymai nebus pakeisti.

XII SKYRIUS

ADMINISTRATORIAUS TEISĖS

64. Administratorius darbo tikslais turi teisę:

64.1. iš anksto neperspėjęs kompiuterio naudotojo prisijungti prie jo kompiuterio darbo vietoje ar nuotoliniu būdu, siekiant užtikrinti jam pavestų funkcijų atlikimą bei užtikrinant kompiuteryje esančios informacijos konfidencialumą;

64.2. įdiegti, pašalinti operacinę sistemą, taikomąją ar kitą Programinę įrangą kompiuterio naudotojo darbo vietoje ar nuotoliniu būdu;

64.3. kopijuoti, išsaugoti ar kitaip panaudoti darbinę informaciją (failus ir kitą informaciją) Centro tikslams be išankstinio kompiuterio naudotojo sutikimo darbo vietoje ar nuotoliniu būdu, užtikrinant tokios informacijos konfidencialumą;

64.4. pastebėjęs veiksmus, galinčius daryti įtaką kompiuterių tinklo ar duomenų saugumui, Kompiuterinės įrangos naudotojui apriboti teises dirbti su jam priskirta Kompiuterine ir Programine įranga. Apie atliktus veiksmus informuojamas Centro ūkvedys ir direktorius. Darbas su Kompiuterine ir Programine įranga atnaujinamas tik pašalinus pastebėtus sutrikimus.

XIII SKYRIUS

ATSAKOMYBĖ UŽ KOMPIUTERINĖS IR PROGRAMINĖS ĮRANGOS NAUDOJIMĄ

65. Materialiai atsakingas darbuotojas yra atsakingas už Kompiuterinės ir Programinės įrangos išdavimą bei priėmimą Centro darbuotojams.

66. Centro darbuotojai privalo saugiai, tinkamai ir ekonomiškai naudoti priskirtą Kompiuterinę ir Programinę įrangą.

67. Darbuotojas materialiai atsako už žalą, padarytą jo tyčiaisiais veiksmais, naudojant jam patiktą kompiuterinę ir kitą IT techniką, įstatymų nustatyta tvarka.

68. Darbuotojas, įstaigos patalpose praradęs jam priskirtą Kompiuterinę ir Programinę įrangą, privalo nedelsdamas apie tai informuoti tiesioginį vadovą.

69. Jei nešiojama Kompiuterinė ir Programinė įranga buvo prarasta ne Centro patalpose, ją praradęs Darbuotojas papildomai turi dėl įvykio kreiptis į policiją.

70. Atleidžiamas iš darbo Darbuotojas jam priskirtą Kompiuterinę ir Programinę įrangą privalo grąžinti materialiai atsakingam darbuotojui.

XIV SKYRIUS

TIEKĖJŲ VALDYMAS

71. Sutartyse su tiekėjais, kuriems yra suteikiama prieiga prie informacijos ir (ar) IT priemonių, turi būti įtraukti informacijos saugumo reikalavimai, susiję su veiklos ir techniniais reikalavimais, įskaitant ir nuostatas dėl konfidencialumo užtikrinimo. Tiekėjams prieiga prie Centro informacinių išteklių gali būti suteikiama tik tokios apimties, kiek tai būtina sutarčiai įgyvendinti ir nedelsiant panaikinama, pasibaigus sutartiniams santykiams.

72. Pasibaigus sutartiniams santykiams iš tiekėjo turi būti reikalaujama grąžinti visą Centro turtą ir gautą informaciją arba sunaikinti ją.

73. Tiekėjų teikiamos paslaugos turi būti stebimos ir kartą per metus turi būti atliekama tiekėjų paslaugų peržiūra, kurios metu atliekamas paslaugų įvertinimas, atsižvelgiant į sutartyse nustatytą informacijos saugumo reikalavimų laikymąsi.

74. Tiekėjų atranka ir vertinimas atliekamas pagal laikantis Lietuvos Respublikos viešųjų pirkimų įstatymo, Lietuvos Respublikos valstybės informacinių išteklių įstatymo 42 punkto ir kitų teisės aktų reikalavimų.

75. Tiekėjai, kuriems sudaroma prieiga prie Centro tvarkomų asmens duomenų, laikomi asmens duomenų tvarkytojais ir tokia prieiga gali būti suteikiama tik Centrai ir Tiekėjui pasirašius sutartį, reglamentuojančią Centro, kaip duomenų valdytojo, ir Tiekėjo, kaip duomenų tvarkytojo, santykius.

XV SKYRIUS KEITIMŲ VALDYMAS

76. Privaloma užtikrinti, kad keitimai būtų valdomi. Keitimų poreikis gali iškilti dėl įvairių priežasčių, įskaitant, bet neapsiribojant žemiau išvardintomis:

- 76.1. naudotojų prašymai;
- 76.2. tiekėjų paslaugų pakeitimai;
- 76.3. esminiai pokyčiai Centre;
- 76.4. techninės ir programinės įrangos atnaujinimai;
- 76.5. naujos techninės ir (ar) programinės įrangos diegimai;
- 76.6. techninės ir (ar) programinės įrangos gedimai;
- 76.7. infrastruktūros pasikeitimai;
- 76.8. nenumatyti įvykiai ir kt.

77. Atsiradus keitimo poreikiui, atsakingas už keitimą Darbuotojas registruoja keitimo datą, iniciatoriaus duomenis, siūlomą pakeitimą, pakeitimo priežastis, reikalingą pakeitimo datą.

78. Atsakingas už keitimą Darbuotojas įvertina tokio keitimo būtinumą ir galimą poveikio mastą bei suderina su Centro ūkvedžiu. Jei keitimo naudos/rizikos santykis yra teigiamas, keitimas tvirtinamas. Jei keitimas gali turėti poveikį kritiniams IT infrastruktūros vienetams, jo įgyvendinimas turi būti testuojamas, numatomi atsitraukimo planai.

79. Ištestavus keitimą, turi būti koordinuojamas jo įgyvendinimas, surenkami keitimui būtini techninės ir programinės įrangos elementai, pasirošama diegimui.

80. Apie keitimus, kurie gali turėti įtaką sistemos darbui, iš anksto, ne vėliau kaip prieš 1 darbo dieną, įspėjami susiję vartotojai.

81. Atliekant keitimą svarbūs sistemos pranešimai turi būti fiksuojami ir žymimi keitimo įrašė.

82. Atlikus keitimą, keitimo įrašė turi būti nurodyta keitimo atlikimo data ir, jei reikia, papildomos pastabos.

83. Po keitimo įgyvendinimo rekomenduojama kurį laiką stebėti konfigūracijos vienetus, kuriems keitimas galėjo turėti įtakos.

84. Didelių keitimų diegimui papildomai taikomos. Dideliais keitimais laikomi:

84.1. visi taikomųjų programų ir jų naujinimų keitimai;

84.2. kiti keitimai, kai:

84.2.1. keletas keitimų yra tarpusavyje susiję, priklauso nuo kitų konfigūracinių vienetų arba gali daryti įtaką kitų konfigūracinių vienetų funkcionavimui;

84.2.2. keitimas yra sudėtingas, jo rizika yra didelė ir reikia šią riziką sumažinti;

84.2.3. keitimas atliekamas daugelyje IT infrastruktūros elementų.

85. Centro ūkvedys, kuris koordinuoja diegimo įgyvendinimą, gavęs diegimo užduotį ją užregistruoja, suformuodamas naują rinkmeną ir įrašo diegimo numerį.

86. Centro ūkvedys, kuris koordinuoja diegimo įgyvendinimą, kartu su kitais Darbuotojais pagal kompetenciją, sudaro diegimo aprašą, kuriame nustatoma diegimo sąranka (diegimą sudarantys konfigūraciniai vienetai ir jų tarpusavio priklausomybė), sąrankos sukūrimo veiksmai, įvertinta diegimo gamybinėje infrastruktūroje rizika ir galimas poveikis IT paslaugoms, sąrankos priimtinumui kriterijai, numatyta diegimo strategija ir tvarkaraštis. Diegimo aprašas teikiamas tvirtinti Centro direktoriui.

87. Pagal nustatytą planą įsigijami, sukuriami, sukonfigūruojami ir /arba išbandomi tęstinėje aplinkoje visi diegimo apraše numatyti IT infrastruktūros elementai (taikomosios programos, operacinės sistemos, kompiuterinė, tinklo įranga ir kt.). Parengiami ar patikslinami eksploataavimo dokumentai. Jei reikia, papildomas ir (arba) patikslinamas diegimo aprašas.

88. Visi diegimai ir jų įgyvendinimas turi būti išbandyti tęstinėje aplinkoje (Centro serveryje ir/arba kompiuterinėje darbo vietoje sukuriama tęstinė aplinka, joje diegiama programinė įranga, jei reikia, vartotojams leidžiama prisijungti prie tęstinės aplinkos ir išbandyti pokyčius).

89. Testavimas vykdomas, vadovaujantis diegimo aprašu, jame nustatyta bandymų tvarka ir priimtino kriterijais.

90. Centro ūkvedys, remdamasis testavimo rezultatais ir įvertinta pokyčių visumos rizika, patvirtina galutinį diegimo aprašą ir autorizuoja diegimą gamybinėje aplinkoje, arba nusprendžia dėl reikalingų papildomų korekcinų veiksmų.

91. Patvirtinta sąranka diegiama gamybinėje aplinkoje (informacinių sistemų serveriuose, darbo vietų kompiuteriuose ir kitose IT infrastruktūros dalyse).

XVI SKYRIUS

INFORMACIJOS APDOROJIMO PRIEMONIŲ NAUDOJIMO STEBĖSENA

92. Informacijos apdorojimo priemonių naudojimo stebėseną vykdoma, reguliariai analizuojant žurnalinius įrašus apie naudotojų atliktus veiksmus bei IT infrastruktūros veikimą, siekiant nustatyti neteisėtus ir/ar neleistinus naudotojų atliekamus veiksmus IT infrastruktūroje, IT infrastruktūros gedimus, klaidas bei potencialius įsilaužimo veiksmus.

93. Vykdoma šių informacijos apdorojimo priemonių naudojimo įvykių stebėseną:

93.1. tarnybinių stočių, informacinės sistemos taikomosios programinės įrangos įjungimas, išjungimas, sėkmingi ir nesėkmingi bandymai registruotis tarnybinėse stotyse, informacinės sistemos taikomojoje programinėje įrangoje;

93.2. naudotojų atliekami veiksmai su valdomų ir (arba) tvarkomų informacinių sistemų ir registro duomenimis (įvedimas, peržiūra, keitimas, naikinimas ir kt.), naudotojų ar jų grupių bei Administratorių teisių naudotis posistemio ištekliais pasikeitimai, audito įrašų trynimai, kūrimas ar keitimas, posistemio parametrų, laiko ir (ar) datos pakeitimai;

93.3. tinklo įrangos įvykiai (analizuojamos ryšio ir tinklo priežiūros paslaugos teikėjo ataskaitos);

93.4. bandymai vykdyti kibernetines atakas (analizuojamos ryšio ir tinklo priežiūros paslaugos teikėjo ataskaitos);

93.5. Administratorių bei IT infrastruktūros priežiūrą vykdančių darbuotojų atliekami veiksmai;

93.6. Programinės įrangos, skirtos apsaugai nuo kenksmingos Programinės įrangos, įvykiai;

93.7. IT infrastruktūros darbiniai parametrų pasikeitimai: procesoriaus apkrovimas, atminties apkrovimas, laisvos diskinės vietos kiekis, pasiekiamumas;

93.8. naudotojo/Administratoriaus ar įrenginio, susijusio su įvykiu, vardas (identifikatorius);

93.9. įvykio rūšis/pobūdis;

93.10. tikslus laikas;

93.11. trukmė;

93.12. įvykio rezultatas;

93.13. kai Darbuotojo daugiau nei 3 darbo dienas dėl nežinomos priežasties nėra darbe arba pasibaigia darbo santykiai, o būtina užtikrinti Centro veiklos tęstinumą;

93.14. Darbuotojo ligos, mirties ar nelaimingo atsitikimo atveju, kai būtina užtikrinti Centro veiklos tęstinumą;

93.15. kai reikia patikrinti informaciją apie Darbuotojo veiksmus, turinčius reikšmės juridinių faktų darbo, civilinės, administracinės ar baudžiamosios teisės šakose (įskaitant teisinius procesus, arbitražą ir pan.) nustatymui ir kurių patvirtinimą ar paneigimą galima įrodyti tik peržiūrint Darbuotojo siųstų arba gautų elektroninių laiškų ir jų priedų turinį;

93.16. kai Centras yra atsakingas už Darbuotojo atliktų veiksmų padarinius ir reikia ginti Centro interesus, siekiant gauti patvirtinimą ar paneigimą dėl galimai neteisėtų Darbuotojo veiksmų;

93.17. kai Darbuotojo veikla galimai neatitinka etiško elgesio normų;

93.18. siekiant patikrinti, kaip Darbuotojai laikosi teisės aktuose ir lokaliuose Centro dokumentuose nustatytų reikalavimų užtikrinant konfidencialios ir padidinto konfidencialumo informacijos ir asmens duomenų apsaugą, apsaugant Centrą nuo šios informacijos neteisėto atskleidimo.

94. Tikrinimo komisija turi teisę peržiūrėti Darbuotojų elektroniniu paštu siųstų ir gautų elektroninių laiškų ir jų priedų turinį vienu iš 105 punkte nustatytu tikslu, tik gavusi motyvuotus rašytinius asmenų (Darbuotojų, trečiųjų asmenų ar institucijų) prašymus, kuriuose privalo būti Centro direktoriaus rezoliucija atlikti Patikrinimą.

95. Centro direktorius, gavęs motyvuotą rašytinį prašymą, atsižvelgdamas į būtinumo, proporcingumo bei teisėtumo principus, rezoliucijoje nurodo, su kiek duomenų leidžiama susipažinti Tikrinimo komisijai, arba priima sprendimą neleisti susipažinti su prašomais duomenimis ir nurodo motyvus.

96. Tikrinimo komisija apie atliktą elektroninio pašto laiškų ir priedų turinio Patikrinimą informuoja tikrintą Darbuotoją, jeigu su juo nėra pasibaigę darbo santykiai, jam pateikia patikrinimo išvadų išrašą, nurodo patikrinimo mastą, išvadas ir/ar rekomendacijas.

97. Tikrinimo komisija, gavusi Centro direktoriaus priimtą rezoliuciją leisti susipažinti su prašomais duomenimis, surenka juos ir pateikia prašomus duomenis tokią teisę turintiems asmenims tokia apimtimi, kuri reikalinga tolimesniems veiksams atlikti, kartu užtikrinant konfidencialios informacijos apsaugą.

98. Tikrinimo komisija pateikia duomenų tik tiek, kiek nurodyta rezoliucijoje, ir baigusi vykdyti užduotį nereikalingą informaciją / duomenis sunaikina. Specializuotų prieigos teisės Tikrinimo komisijos nariams prie elektroninio pašto duomenų suteikiamos bendra prieigos suteikimo tvarka.

99. Tikrinimo komisija atlikdama Darbuotojų naudojamo elektroninio pašto laiškų ir jų priedų patikrinimą turi teisę gauti Darbuotojų paaiškinimus, jeigu su Darbuotojais nėra pasibaigę darbo santykiai. Tikrinimo komisija, peržiūrėjusi elektroninio pašto laiškų ir jų priedų turinį, reikalingus duomenis naudoja tyrimui užtikrinti.

100. Tikrinimo komisija privalo saugoti konfidencialią ir padidinto konfidencialumo informaciją ir asmens duomenis, su kuriais susipažino atlikdami Darbuotojų elektroninio pašto laiškų ir jų priedų Patikrinimą, ir neatskleisti jų šiame Apraše nenurodytais tikslais.

101. Darbuotojų elektroninio pašto duomenų srautai, susirašinėjimo turinys, įskaitant pridedamus elektroninio laiško dokumentus, kopijuojami ir saugomi 5 (penkerius) metų nuo laiškų gavimo (siuntimo) momento. Už nurodytos informacijos išsaugojimą atsakingas Centro vadovas.

102. Centro išeinančių ir įeinančių elektroninio pašto laiškų gavėjai turi būti informuoti, kad Centro elektroninio pašto srauto duomenys, susirašinėjimo turinys, įskaitant pridedamus elektroninio laiško dokumentus, kopijuojami ir saugomi 5 (penkerius) metų nuo laiškų gavimo ir, vadovaujantis šio Aprašo nustatytais pagrindais ir atvejais, gali būti atliktas elektroninio pašto laiškų ir jų priedų Patikrinimas.

XVII SKYRIUS

ĮRANGOS IR INFORMACIJOS NAIKINIMAS, TAISYMAS IR PAKARTOTINIS NAUDOJIMAS

103. Kompiuterinė įranga nurašoma bendra Centro ilgalaikio turto nurašymo tvarka.

104. Už nurašytos Kompiuterinės įrangos utilizavimą atsakingas Centro ūkvedys.

105. Gavęs nurašytos technikos sąrašą, Centro ūkvedys privalo:

105.1. sutvarkyti duomenų laikmenas, t. y. mechaniškai sugadinti laikmeną arba suformatuoti, naudojant specializuotą Programinę įrangą, kuri užkirstų kelią atstatyti duomenis;

105.2. suorganizuoti Kompiuterinės įrangos išvežimą į utilizavimu užsiimančią įmonę;

105.3. pristatyti į buhalteriją pažymą apie priduoatą įrangą.

106. Nebereikalinga popierinė informacija turi būti naikinama dokumentų naikikliu, o elektroninė – programinėmis priemonėmis tokiu būdu, kad jos nebūtų galima atkurti.

107. Panaudojant Kompiuterinę įrangą pakartotinai, turi būti atliktas duomenų perrašymas.

108. Sugedusią Kompiuterinę įrangą Darbuotojai turi atiduoti atsakingam Centro ūkvedžiui, kuris rūpinasi saugiu įrangos naikinimu arba taisymu ir užtikrina, kad nebūtų galimybės neleistinai prieigai prie Kompiuterinės įrangos.

109. Atiduodant taisyti sugedusią įrangą iš jos turi būti išimamos atmintinės, kuriose gali būti svarbios informacijos.

XVIII SKYRIUS BAIGIAMOSIOS NUOSTATOS

110. Darbuotojai, pažeidę šios tvarkos nuostatas atsako Lietuvos Respublikos įstatymų ir kitų teisės aktų nustatyta tvarka.

111. Visi kiti šiame Apraše nenumatyti veiksmai, susiję su Kompiuterinės ir Programinės įrangos naudojimu Centre privalo būti derinami su Centro direktoriumi.

112. Išimtys valdomos pagal Informacijos saugumo išimčių valdymo procedūrą. Lietuvos Respublikos Vyriausybės 2003 m. balandžio 18 d. nutarimu Nr. 480 „Dėl bendrųjų reikalavimų valstybės ir savivaldybių institucijų ir įstaigų interneto svetainėms aprašo patvirtinimo“.
