PATVIRTINTA
Valstybės garantuojamos teisinės pagalbos tarnybos direktoriaus 2021 m. liepos 15 d. įsakymu Nr. (1.2)V-8

VALSTYBĖS GARANTUOJAMOS TEISINĖS PAGALBOS TARNYBOS INFORMACINIŲ SISTEMŲ DUOMENŲ SAUGOS NUOSTATAI

I. BENDROSIOS NUOSTATOS

1. Valstybės garantuojamos teisinės pagalbos tarnybos (toliau – Tarnyba) informacinių sistemų duomenų saugos nuostatai (toliau – Saugos nuostatai) nustato principus ir reikalavimus, užtikrinančius saugų elektroninės informacijos tvarkymą automatiniu būdu (toliau – Saugos politika) Tarnybos informacinėse sistemose, jų posistemiuose ir duomenų rinkmenose (toliau – IS) atliekant Tarnybai pavestas funkcijas.

2. Tarnybos IS duomenų Saugos nuostatai taikomi visoms, Tarnybos pagal Lietuvos Respublikos teisės aktus tvarkomoms duomenų grupėms ir visoms Tarnyboje naudojamoms įdiegtoms ir ateityje diegiamoms IS.

3. Saugos nuostatuose vartojamos sąvokos suprantamos taip, kaip jos apibrėžtos Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatyme, Lietuvos Respublikos kibernetinio saugumo įstatyme, Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 patvirtintuose Bendrajame elektroninės informacijos saugos reikalavimų apraše, Saugos dokumentų turinio gairių apraše ir Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių apraše (toliau bendrai vadinama – Aprašas) ir kituose teisės aktuose bei Lietuvos standartuose LST ISO/IEC 27001:2013 ir LST ISO/IEC 27002:2014.

4. Už Tarnyboje naudojamų IS elektroninės informacijos valdymo/tvarkymo teisėtumą ir elektroninės informacijos saugą atsako Tarnyba.

5. Tarnyba užtikrina IS elektroninės informacijos saugumą, vientisumą, konfidencialumą, prieinamumą, tinkamą kompiuterių bei komunikacinės įrangos funkcionavimą administracijoje ir IS duomenų teikimą IS duomenų gavėjams.

6. Tarnyba, vadovaudamasi Saugos nuostatais, skiria IS saugos įgaliotinį (toliau – Saugos įgaliotinis), esant poreikiui IS duomenų valdytojus/tvarkytojus, sudaro elektroninės informacijos saugos darbo grupes, viešųjų pirkimų įstatymo nustatyta tvarka įsigyja IS administratoriaus funkcijas atliekančių fizinių ar juridinių asmenų paslaugas.

7. Tarnybos elektroninės informacijos saugumo užtikrinimo tikslai:

7.1. informacijos patikimumo, vientisumo, konfidencialumo, prieinamumo ir saugumo užtikrinimas;

7.2. kompiuterizuotų darbo vietų tinkamo saugumo lygio įdiegimas ir palaikymas;

7.3. nuolatinis vietinio kompiuterių tinklo funkcionavimo užtikrinimas bei saugumo stebėsena;

7.4. tinkamo kompiuterinės, programinės ir tinklo įrangos funkcionavimo ir saugumo užtikrinimas.

8. Saugos nuostatai privalomi visiems IS naudotojams.

9. Tarnybos direktoriaus tvirtinamos saugaus elektroninės informacijos tvarkymo taisyklės, IS veiklos tęstinumo valdymo planas ir IS naudotojų administravimo taisyklės yra duomenų saugos nuostatuose nustatytą duomenų Saugos politiką įgyvendinantys teisės aktai.

10. Tarnybos elektroninės informacijos saugumo užtikrinimo prioritetinės kryptys**:**

10.1. elektroninės informacijos konfidencialumo užtikrinimas;

10.2. elektroninės informacijos prieinamumo užtikrinimas;

10.3. elektroninės informacijos vientisumo užtikrinimas;

10.4. veiklos tęstinumo užtikrinimas;

10.5. asmens duomenų apsauga.

11. Kiekvienas IS naudotojas tvarko tik tą elektroninę informaciją, kuri jam prieinama naudojant konkrečios IS programinę įrangą.

12. IS valdytojas/tvarkytojas – Tarnyba, įsikūrusi Odminių g. 3, Vilnius.

13. IS duomenų valdytojo/tvarkytojo funkcijos ir atsakomybė:

13.1. pagal kompetenciją atsako už elektroninės informacijos saugą;

13.2. rengia IS kūrimo ir plėtros planus;

13.3. prižiūri IS kūrimą, diegimą ir tvarkymą;

13.4. kontroliuoja lėšų, skirtų IS, panaudojimą;

13.5. kontroliuoja, kad IS būtų tvarkoma vadovaujantis Lietuvos Respublikos įstatymais, Saugos nuostatais ir kitais Saugos politiką įgyvendinančiais teisės aktais;

13.6. rengia ir priima teisės aktus, susijusius su IS veikla ir duomenų sauga, organizuoja jų įgyvendinimą.

14. IS valdytojas rengia ir tvirtina šiuos Saugos politiką įgyvendinančius dokumentus:

14.1. saugaus IS elektroninės informacijos tvarkymo taisykles;

14.2. IS veiklos tęstinumo valdymo planą;

14.3. IS naudotojų administravimo taisykles.

15. IS valdytojo vadovas sprendimu paskiria IS saugos įgaliotinį ir viešųjų pirkimų įstatymo nustatyta tvarka vykdant mažos vertės pirkimą pagal paslaugų teikimo sutartį įsigyja informacinių sistemų aptarnavimo paslaugas, iš fizinių ar juridinių asmenų kurie ir priskiriami IS administratoriumi.

16. Saugos įgaliotinis organizuoja ir kontroliuoja šių Saugos nuostatų įgyvendinimą ir atlieka šias funkcijas:

16.1. teikia IS valdytojui pasiūlymus dėl:

16.1.1. IS administratorių skyrimo;

16.1.2. Saugos politiką įgyvendinančių dokumentų priėmimo, keitimo ar panaikinimo;

16.2. IS saugos reikalavimų atitikties vertinimo atlikimo;

16.3. koordinuoja elektroninės informacijos saugos incidentų, įvykusių IS, tyrimą;

16.4. duoda IS administratoriams privalomus vykdyti nurodymus;

16.5. teisės aktų nustatyta tvarka atlieka IS saugos atitikties vertinimą. Jei vertinimui atlikti būtina įsigyti vertinimo paslaugas, teikia IS valdytojui pasiūlymus dėl minėtų paslaugų įsigijimo;

16.6. atlieka kitas IS valdytojo vadovo ar jo įgalioto asmens pavestas ir šiais saugos nuostatais jam priskirtas funkcijas.

17. IS administratoriaus funkcijos ir atsakomybė:

17.1. atsako už priskirtos IS funkcionavimą, IS naudotojų registravimą ir registravimosi vardų skyrimą, prieigos prie IS teisių nustatymą;

17.2. įvertina IS naudotojų pasirengimą dirbti su IS;

17.3. rengia pasiūlymus dėl IS kūrimo, palaikymo, priežiūros ir duomenų saugos;

17.4. atlieka IS sudarančių komponentų (kompiuterių, operacinių sistemų, duomenų bazių valdymo sistemų, taikomųjų programų sistemų, ugniasienių, duomenų perdavimo tinklų) administravimą, pažeidžiamų vietų ir saugos reikalavimų atitikties nustatymą;

17.5. registruoja elektroninės informacijos saugos incidentus ir informuoja apie juos saugos įgaliotinį, teikia pasiūlymus dėl minėtų incidentų pašalinimo;

17.6. tvarkydami IS elektroninę informaciją neatskleidžia, neperduoda tvarkomos informacijos nė vienam asmeniui, kuris nėra įgaliotas naudotis šia informacija tiek administracijoje, tiek už jos ribų;

17.7. jei IS tvarkomi asmens duomenys, saugo asmens duomenų paslaptį;

17.8. neperduoda neįgaliotiems asmenimis slaptažodžių, naudotojo tapatybės kodų ar kitos informacijos, leidžiančios naudojantis programinėmis ir techninėmis priemonėmis sužinoti

asmens duomenis ar kitą IS tvarkomą elektroninę informaciją, ir nesudaro kitų sąlygų susipažinti su IS tvarkoma elektronine informacija;

17.9. atlieka kitas šiuose Saugos nuostatuose ir kituose Saugos politiką įgyvendinančiuose dokumentuose priskirtas funkcijas ir vykdo kitus IS valdytojo/tvarkytojo ar saugos įgaliotinio nurodymus, susijusius su IS sauga.

18. IS naudotojų funkcijos ir atsakomybė:

18.1. vadovaudamiesi IS valdytojo/tvarkytojo patvirtintais Saugos nuostatais, IS naudojimo instrukcijomis ir pareigybių aprašymais, naudoja IS;

18.2. tvarko IS elektroninę informaciją ir naudojasi kitomis Tarnybos IS teikiamomis galimybėmis pagal nustatytą funkcijoms atlikti reikalingą IS prieigos teisių lygmenį, kuris apriboja naudojimosi elektronine informacija apimtį;

18.3. pagal kompetenciją rengia pasiūlymus dėl IS kūrimo, palaikymo, priežiūros ir elektroninės informacijos saugos;

18.4. tvarkydami IS elektroninę informaciją neatskleidžia, neperduoda tvarkomos informacijos nė vienam asmeniui, kuris nėra įgaliotas naudotis šia informacija;

18.5. jei IS tvarkomi asmens duomenys, saugo asmens duomenų paslaptį;

18.6. neperduoda neįgaliotiems asmenimis slaptažodžių, naudotojo tapatybės kodų ar kitos informacijos, leidžiančios naudojantis programinėmis ir techninėmis priemonėmis sužinoti asmens duomenis ar kitą IS tvarkomą elektroninę informaciją, ir nesudaro kitų sąlygų susipažinti su IS tvarkoma elektronine informacija;

18.7. vykdo kitas šiuose Saugos nuostatuose ir Saugos politiką įgyvendinančiuose dokumentuose priskirtas funkcijas.

19. Tvarkant IS elektroninę informaciją bei rengiant saugos politiką įgyvendinančius dokumentus, vadovaujamasi:

19.1. Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymu;

19.2. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymu;

19.3. Lietuvos Respublikos kibernetinio saugumo įstatymu;

19.4. Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo patvirtinimo“;

19.5. Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašu, patvirtintu Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“;

19.6. Techninių valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimų aprašu, patvirtintu Lietuvos Respublikos krašto apsaugos ministro 2020 m. gruodžio 4 d. įsakymu Nr. V-941 „Dėl Techninių valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimų aprašo ir Informacinių technologijų saugos atitikties vertinimo metodikos patvirtinimo“;

19.7. Lietuvos standartais LST ISO/IEC 27001:2013 ir LST ISO/IEC 27002:2014, taip pat kitais Lietuvos ir tarptautiniais grupės „Informacijos technologija. Saugumo metodai“ standartais;

19.8. 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentu (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas);

19.9. kitais teisės aktais, kuriais reglamentuojamas elektroninės informacijos tvarkymo teisėtumas, IS valdytojo/tvarkytojo veikla ir elektroninės informacijos saugos valdymas.

II. ELEKTRONINĖS INFORMACIJOS SAUGOS VALDYMAS

20. Vadovaujantis Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo, patvirtinto Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo patvirtinimo“, 9.2 ir 9.5 papunkčiais, Sistemose tvarkoma informacija priskiriama vidutinės svarbos informacijos kategorijai.

21. Vadovaujantis Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo, patvirtinto Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo patvirtinimo“, 12.3 papunkčiu, IS priskiriamas trečiajai informacinių sistemų kategorijai.

22. Informacinės sistemos saugos įgaliotinis, atsižvelgdamas į Nacionalinio kibernetinio saugumo centro svetainėje skelbiamą metodinę priemonę „Rizikos analizės vadovas“, kasmet organizuoja Informacinės sistemos rizikos įvertinimą. Pasikeitus Informacinės sistemos duomenų bazės struktūrai (sistemos pakeitimai, papildymas naujomis taikomosiomis programomis, taikomųjų programų pašalinimas ir kt.) ar po esminių organizacinių ar sisteminių pokyčių, nustačius naujų rizikos veiksnių, gali būti organizuojamas neeilinis Informacinės sistemos rizikos įvertinimas. Informacinės sistemos rizikos vertinimas gali būti atliekamas kartu su informacinių technologijų saugos atitikties vertinimu.

23. IS rizikos įvertinimo rezultatai išdėstomi rizikos įvertinimo ataskaitoje, kuri pateikiama IS valdytojo vadovui. Rizikos įvertinimo ataskaita rengiama įvertinant rizikos veiksnius, galinčius turėti įtakos elektroninės informacijos saugai, jų galimą žalą, pasireiškimo tikimybę ir pobūdį, galimus rizikos valdymo būdus, rizikos priimtinumo kriterijus. Svarbiausieji rizikos veiksniai yra šie:

23.1. subjektyvūs netyčiniai (elektroninės informacijos tvarkymo klaidos ir apsirikimai, elektroninės informacijos ištrynimas, klaidingas elektroninės informacijos teikimas, fiziniai elektroninės informacijos technologijų sutrikimai, elektroninės informacijos perdavimo tinklų sutrikimai, programinės įrangos klaidos, neteisingas veikimas ir kita);

23.2. subjektyvūs tyčiniai (nesankcionuotas naudojimasis IS elektroninei informacijai gauti, elektroninės informacijos pakeitimas ar sunaikinimas, informacinių technologijų duomenų perdavimo tinklais sutrikdymai, saugumo pažeidimai, vagystės ir kita);

23.3. veiksniai, nurodyti Atleidimo nuo atsakomybės esant nenugalimos jėgos (*force majeure*) aplinkybėms taisyklių, patvirtintų Lietuvos Respublikos Vyriausybės 1996 m. liepos 15 d. nutarimu Nr. 840 „Dėl Atleidimo nuo atsakomybės esant nenugalimos jėgos *(force majeure)* aplinkybėms taisyklių patvirtinimo“, 3 punkte.

24. IS elektroninei informacijai, techninei, programinei įrangai, patalpoms IS valdytojo/tvarkytojo įstaigoje vertinti naudojama penkiabalė rizikos veiksnių tikimybės ir žalos vertinimo metodika:

24.1. nereikšminga rizikos veiksnių tikimybė, žala – 1 balas;

24.2. maža rizikos veiksnių tikimybė, žala – 2 balai;

24.3. vidutinė rizikos veiksnių tikimybė, žala – 3 balai;

24.4. didelė rizikos veiksnių tikimybė, žala – 4 balai;

24.5. labai didelė rizikos veiksnių tikimybė, žala – 5 balai.

25. IS rizikos vertinimo metu atliekami darbai:

25.1. IS sudarančių informacinių išteklių inventorizacija;

25.2. įtakos IS veiklai vertinimas;

25.3. grėsmės ir pažeidimų analizė;

25.4. liekamosios rizikos vertinimas;

26. Atsižvelgdamas į IS rizikos įvertinimo ataskaitą, Tarnybos vadovas prireikus tvirtina rizikos įvertinimo ir rizikos valdymo priemonių planą, kuriame numatomas techninių, administracinių ir kitų išteklių poreikis rizikos valdymo priemonėms įgyvendinti.

27. Pagrindiniai IS duomenų saugos priemonių parinkimo principai yra šie:

27.1. likutinė rizika turi būti sumažinama iki priimtino lygio;

27.2. duomenų saugos priemonės diegimo kaina turi būti adekvati saugomų duomenų vertei;

27.3. kur galima, turi būti įdiegiamos prevencinės, detekcinės ir korekcinės duomenų saugos priemonės.

28. Kartą per dvejus metus atliekamas IS saugos atitikties vertinimas, kurio metu:

28.1. įvertinama Saugos politikos dokumentų ir realios informacijos saugos situacijos atitiktis;

28.2. inventorizuojama IS techninė ir programinė įranga;

28.3. patikrinama ne mažiau kaip 10 procentų atsitiktinai parinktų IS naudotojų kompiuterinių darbo vietų, tarnybinėse stotyse įdiegtų programų ir jų sąranka;

28.4. įvertinama ne mažiau kaip 10 procentų atsitiktinai parinktų IS naudotojų suteiktų teisių atitiktis vykdomoms funkcijoms;

28.5. įvertinamas pasirengimas užtikrinti IS veiklos tęstinumą įvykus saugos incidentui.

29. Atlikus šių nuostatų 28 punkte nurodytą vertinimą, rengiamas pastebėtų trūkumų šalinimo planas, kurį tvirtina, atsakingus vykdytojus paskiria ir įgyvendinimo terminus nustato IS valdytojas/tvarkytojas.

30. Neeilinis IS rizikos vertinimas turi būti atliekamas:

30.1. įvykus pokyčiams IS techninėje ar programinėje įrangoje, kurie galėtų įtakoti IS veikimą;

30.2. paaiškėjus naujoms tendencijoms informacinių technologijų saugos srityje, dėl kurių kiltų grėsmė IS techninei, programinei įrangai ar IS tvarkomiems duomenims;

30.3. po saugos incidento, kurio metu būtų sutrikdyta IS veikla, sugadinti ar prarasti IS duomenys.

31. IS sauga turi būti įgyvendinama siekiant išsaugoti IS elektroninės informacijos savybes. Pirmiausia turi būti diegiamos priemonės, skirtos išsaugoti toms elektroninės informacijos savybėms, kurių praradimas turėtų didžiausią įtaką IS darbui.

32. Pasirenkant saugos priemones prioritetas teikiamas toms priemonėms, kurių diegimas reikalauja mažiausiai sąnaudų ir duoda didžiausią efektą.

33. Informacinės sistemos rizikos įvertinimo ataskaitos, Informacinės sistemos rizikos įvertinimo ir rizikos valdymo priemonių plano, Informacinės sistemos informacinių technologijų saugos atitikties vertinimo ataskaitos, taip pat pastebėtų trūkumų šalinimo plano kopijas Informacinės sistemos valdytojas ne vėliau kaip per 5 darbo dienas nuo minėtų dokumentų priėmimo turi pateikti Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemai Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemos nuostatų, patvirtintų Lietuvos Respublikos krašto apsaugos ministro 2018 m. gruodžio 11 d. įsakymu Nr. V-1183 „Dėl Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemos nuostatų patvirtinimo“, nustatyta.

III. ORGANIZACINIAI IR TECHNINIAI REIKALAVIMAI

34. Organizacinių ir techninių elektroninės informacijos saugos (kibernetinio saugumo) priemonių užtikrinimas turi būti grindžiamas grėsmių ir pažeidžiamumų, galinčių turėti įtakos IS

elektroninės informacijos saugai (kibernetiniam saugumui), rizikos vertinimu, atsižvelgiant į naujausius technikos laimėjimus.

35. IS serverių apsauga nuo kenksmingos programinės įrangos (virusų, programinės įrangos, skirtos šnipinėti, nepageidaujamo elektroninio pašto ir pan.) užtikrinama programinėmis priemonėmis. Antivirusinė programinė įranga turi būti atnaujinama ne rečiau kaip kartą per 24 valandas.

36. IS tarnybinėse stotyse ir kompiuterinėse darbo vietose nustatomas automatinis operacinės sistemos atnaujinimas atliekamas pagal techninės ir programinės įrangos gamintojo rekomendacijas.

37. IS funkcionuoti būtina programinė tarnybinių stočių ir kompiuterinėse darbo vietose esanti programinė įranga (operacinės sistemos, duomenų bazių ir aplikacijų valdymo programinė įranga, interneto naršyklės, interneto naršyklių priedai ir kt.) turi būti konfigūruojama laikantis programinės įrangos gamintojų saugaus konfigūravimo rekomendacijų.

38. Programinės įrangos diegimą, šalinimą ir konfigūravimą atlieka IS administratorius. Programinės įrangos konfigūravimas yra apsaugotas slaptažodžiu.

39. IS darbo vietose draudžiama naudoti programinę įrangą, nesusijusią su IS naudotojų tiesiogine veikla ir funkcijomis.

40. IS objektų duomenims saugiai rinkti, apdoroti, kaupti, saugoti, teikti informacinėms sistemoms, suinteresuotiems fiziniams ir juridiniams asmenims IS naudotojai turi naudoti programinės ir techninės įrangos saugos priemones, kuriose ne mažiau kaip:

40.1. realizuota galimybė IS naudotojams naudoti tik legalią programinę įrangą;

40.2. realizuota IS naudotojams prieigos prie IS duomenų galimybė tik per registravimosi ir slaptažodžių sistemą;

40.3. realizuota prievolė IS naudotojams reguliariai keisti slaptažodžius;

40.4. realizuota galimybė identifikuoti IS naudotojus, fiksuoti ir kaupti jų duomenų tvarkymo veiksmus;

40.5. realizuota galimybė IS naudotojų užklausas į IS duomenų bazę fiksuoti programiniu būdu;

40.6. apribotas programinės įrangos, nesusijusios su IS naudotojų funkcijomis (žaidimai, internetinės programos ir kt.), naudojimas;

41. Prieigos prie IS užtikrinimo metodai ir priemonės:

41.1. IS duomenys prieinami iš vidinio Tarnybos tinklo visą parą;

41.2. prieigos prie IS elektroninės informacijos teises gali suteikti tik IS administratorius.

41.3. teisė dirbti su konkrečiais IS duomenimis suteikiama konkrečiam IS naudotojui arba IS naudotojų grupei;

41.4. IS veiklos tęstinumui užtikrinti IS duomenys yra periodiškai kas 24 valandos kopijuojami į rezervinių kopijų laikmenas ir laikmenos saugomos taip, kad kilus elektroninės informacijos saugos incidentui IS veiklą iš atsarginių kopijų būtų galima atkurti per 16 darbo valandų. Bylų mėnesinių kopijų laikmenos turi būti laikomos atskiroje patalpoje.

41.5. pasibaigus IS naudotojo darbo sutarčiai, teisė naudotis IS elektronine informacija turi būti panaikinta. IS naudotojui prieiga prie IS turi būti ribojama ar sustabdoma, kai vyksta IS naudotojo veiklos tyrimas, naudotojas turi ilgalaikes atostogas arba keičiasi jo atliekamos ir (ar) pareigybės aprašyme nurodytos funkcijos.

42. IS naudotojams, savo tarnybinėms ir darbo funkcijoms vykdyti naudojantiems nešiojamuosius ir stacionarius kompiuterius, IS duomenims perduoti kompiuterių tinklais ne savo darbo vietoje turi būti naudojamas kompiuterio įjungimo slaptažodis, papildomas IS naudotojo tapatybės patvirtinimas ir IS duomenų šifravimas.

43. IS tarnybinių stočių infrastruktūra turi būti pajungta prie interneto naudojant ugniasienes. Ugniasienių sąranka turi būti nustatyta taip, kad jos praleistų tiktai IS veikimui reikalingą elektroninių duomenų srautą.

44. Prieiga prie kompiuterių ir tarnybinių stočių operacinių sistemų valdymo ir konfigūravimo leidžiama tik administratoriui, atsakingam už kompiuterių tinklo filtravimo įrangos (užkardų, turinio kontrolės sistemų, įgaliotojų serverių) administravimą ir priežiūrą.

45. IS naudotojai gali naudotis tik tomis IS posistemėmis ir jose apdorojamais duomenimis, prie kurių prieiga jiems yra numatyta pagal vykdomas pareigas ir tokią prieigą suteikė saugos įgaliotinis ir administratorius.

46. Dėl IS sutrikimų, neįprasto jos veikimo, esamų arba galimų informacijos saugos reikalavimų pažeidimų ar kitų darbuotojų nederamų veiksmų vartotojai nedelsdami privalo kreiptis į administratorių.

47. IS naudotojų darbo su IS duomenimis tvarką nustato šie nuostatai.

48. IS duomenys perduodami automatiniu būdu naudojant saugų valstybinį duomenų perdavimo tinklą pagal IS duomenų teikimo sutartis, kuriose nustatytos perduodamų duomenų specifikacijos, perdavimo sąlygos ir tvarka.

49. IS naudotojų darbo vietose naudojama programinė įranga, skirta apsaugoti naudotojų darbo vietas nuo kenksmingos programinės įrangos (virusų, programinės įrangos, skirtos šnipinėti, nepageidaujamo elektroninio pašto ir pan.). Ši programinė įranga turi būti atnaujinama ne rečiau kaip vieną kartą per savaitę.

50. IS naudotojams, kuriems atliekant tiesiogines pareigas būtina prisijungti iš nutolusios darbo vietos, gali būti suteikiama nuotolinio prisijungimo prie IS galimybė:

50.1. techninis nuotolinio prisijungimo sprendimas turi užtikrinti ne žemesnį nei vidiniam prisijungimui naudojamą saugumo lygį, t. y. turi būti naudojamos Saugos nuostatuose nurodytos priemonės ir elektroninės informacijos šifravimas naudojantis virtualiu privačiu tinklu (angl. virtual private network – VPN);

50.2. prie IS prisijungiama nuotoliniu būdu naudojant interneto naršyklę (HTTPS protokolą).

51. Leistinos kompiuterių, planšečių ir kitų mobiliųjų įrenginių naudojimo ribos:

51.1. IS duomenų tvarkymui leidžiama naudoti tik leistinus stacionarius ir nešiojamuosius kompiuterius, atitinkančius IS valdytojo nustatytus elektroninės informacijos saugos ir kibernetinio saugumo reikalavimus;

51.2. įrenginiuose turi būti užtikrintas darbuotojo tapatybės autentifikavimas, kiekvieno prisijungimo prie įrenginio metu įvedant vartotojo vardą ir slaptažodį.

51.3. stacionarūs ir nešiojamieji IS naudotojų kompiuteriai ir kiti mobilieji įrenginiai turi būti naudojami tik tiesioginėms pareigoms atlikti. Iš įrenginių, kurie perduodami remontuoti ar techninei priežiūrai atlikti, turi būti pašalinti visi IS duomenys ir informacija.

51.4. nešiojamuosiuose kompiuteriuose ir kituose mobiliuosiuose įrenginiuose turi būti taikomos papildomos saugos priemonės – duomenų šifravimas, prisijungimo ribojimas, papildomas tapatybės patvirtinimas, rakinimo įrenginių naudojimas.

51.5. įrenginiuose neturi būti jokios svarbios informacijos, išskyrus naudotojo darbo dokumentus.

51.6. IS naudotojai privalo naudotis visomis saugumo priemonėmis, kad apsaugotų įrenginius ir duomenų laikmenas nuo vagystės arba pažeidimo.

52. Pagrindiniai atsarginių duomenų kopijų darymo ir atkūrimo reikalavimai:

52.1. atsarginės duomenų bazių kopijos daromos periodiškai, automatiniu būdu.

52.2. prireikus atkurti kopijas turi teisę tik sisteminės priežiūros ir tvarkymo administratorius ar jį pavaduojantis asmuo. Kopijų darymo ir saugojimo tvarka nustatoma IS saugaus elektroninės informacijos tvarkymo taisyklėse.

52.3. atsarginių kopijų laikmenos turi būti pažymimos taip, kad jas būtų galima atpažinti.

52.4. už atsarginių duomenų kopijų darymo ir atkūrimo, taikomosios programinės įrangos (aplikacijų) kopijų darymo vykdymą atsakingas IS administratorius.

52.5. atsarginės duomenų kopijos turi būti saugomos užrakintoje nedegioje spintoje, kitose patalpose.

53. Atsarginių kopijų darymas turi užtikrinti IS duomenų bazės tęstinumą.

54. Elektroninės informacijos atkūrimo iš atsarginių kopijų testavimas turi būti atliekamas ne rečiau kaip kartą per metus.

IV. REIKALAVIMAI PERSONALUI

55. IS naudotojai turi turėti naudojimosi kompiuteriu įgūdžių, būti susipažinę su Saugos nuostatais ir kitais IS saugos dokumentais.

56. IS administratoriumi gali būti įmonė, pasirašiusi paslaugų teikimo sutartį, išmananti darbą su kompiuterių tinklais ir mokanti užtikrinti jų saugumą.

57. IS administratorius privalo sugebėti užtikrinti informacinės sistemos techninės ir programinės įrangos nepertraukiamą funkcionalumą, mokėti administruoti ir prižiūrėti duomenų bazes, stebėti techninės ir programinės įrangos veikimą, atlikti techninės ir programinės įrangos profilaktinę priežiūrą, sutrikimų diagnostiką ir šalinimą, išmanyti elektroninės informacijos saugos principus, turi būti susipažinęs su Saugos nuostatais bei kitais Saugos politiką įgyvendinančiais dokumentais.

58. IS saugos įgaliotinis privalo išmanyti pagrindinius Saugos politikos, darbo su duomenų perdavimo tinklais, jų saugumo užtikrinimo principus ir priemones savo darbe vadovautis Aprašo, kitų Lietuvos Respublikos ir Europos Sąjungos teisės aktų nuostatomis.

59. IS naudotojų ir IS administratorių mokymo planavimo, organizavimo ir vykdymo tvarka, mokymo periodiškumo reikalavimai:

59.1. IS naudotojams turi būti įvairiais būdais primenama apie elektroninės informacijos saugos (kibernetinio saugumo) problemas (pvz., priminimai elektroniniu paštu, teminių renginių organizavimas, atmintinės naujiems IS naudotojams, IS administratoriui ir pan.);

59.2. 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), saugos įgaliotinio, IS naudotojų ar IS administratoriaus poreikius;

59.3. 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.);

59.4. mokymai IS naudotojams turi būti organizuojami periodiškai, bet ne rečiau kaip kartą per metus. Už mokymų organizavimą atsakingas IS saugos įgaliotinis. Mokymai IS saugos įgaliotiniui ir IS administratoriui turi būti organizuojami pagal poreikį.

V. INFORMACINĖS SISTEMOS NAUDOTOJŲ SUPAŽINDINIMO SU SAUGOS DOKUMENTAIS PRINCIPAI

60. IS naudotojai privalo rūpintis IS bei joje tvarkomų duomenų saugumu.

61. IS saugos įgaliotinis ir jo pavedimu IS administratorius yra atsakingi už IS naudotojų supažindinimą su Saugos nuostatais ir kitais Saugos politiką įgyvendinančiais teisės aktais, reglamentuojančiais IS duomenų tvarkymą ir elektroninės informacijos saugą, taip pat supažindina IS naudotojus su atsakomybe už minėtų reikalavimų nesilaikymą.

62. IS naudotojų supažindinimas su IS duomenų Saugos politika ir ją įgyvendinančiais dokumentais registruojamas žurnale, kurio forma nustatyta Saugos nuostatų 1 priede.

63. IS naudotojai su Saugos nuostatais ir kitais Saugos politiką įgyvendinančiais dokumentais bei atsakomybe už šių reikalavimų nesilaikymą supažindinami pasirašytinai. Už IS naudotojų supažindinimo su duomenų Saugos politika ir ją įgyvendinančiais dokumentais žurnalo pildymą atsakingas IS saugos įgaliotinis.

VI. BAIGIAMOSIOS NUOSTATOS

64. Saugos įgaliotinis organizuoja IS saugos dokumentų peržiūrą ne rečiau kaip kartą per metus. Saugos dokumentai turi būti peržiūrimi atlikus rizikos įvertinimą ar informacinių technologijų saugos atitikties vertinimą, įvykus esminiams organizaciniams, sisteminiams ar kitiems pokyčiams.

65. IS naudotojai, administratoriai ar saugos įgaliotinis, pažeidę IS saugos dokumentų nuostatas, atsako Lietuvos Respublikos įstatymų nustatyta tvarka.

_____

Valstybės garantuojamos teisinės pagalbos tarnybos informacinės sistemos duomenų saugos nuostatų 1 priedas

VALSTYBĖS GARANTUOJAMOS TEISINĖS PAGALBOS TARNYBOS INFORMACINĖS SISTEMOS NAUDOTOJŲ SUPAŽINDINIMO SU SAUGOS POLITIKA IR JĄ ĮGYVENDINANČIAIS DOKUMENTAIS ŽURNALAS

Eil. Nr.	Supažindinimo data	IS naudotojo vardas, pavardė	IS naudojo pareigos	Parašas
1.				
2.				
3.				
4.				
5.				
6.				
7.				
8.				
9.				
10.				