PATVIRTINTA
Lietuvos Respublikos aplinkos ministro
2011 m. d. įsakymu Nr.

LIETUVOS RESPUBLIKOS APLINKOS MINISTERIJOS INFORMACINIŲ SISTEMŲ SAUGAUS ELEKTRONINĖS INFORMACIJOS TVARKYMO TAISYKLĖS

I. BENDROSIOS NUOSTATOS

1. Lietuvos Respublikos aplinkos ministerijos (toliau – Ministerija) informacinių sistemų saugaus elektroninės informacijos tvarkymo taisyklės (toliau – Taisyklės) nustato tvarką, užtikrinančią saugų informacinių sistemų techninės ir programinės įrangos funkcionavimą, duomenų tvarkymą ir reikalavimus valstybės tarnautojams ir darbuotojams, dirbantiems pagal darbo sutartis, tiesioginių pareigų vykdymui naudojantiems šias informacines sistemas: Aplinkos informacijos valdymo integruota kompiuterinė sistema, Aplinkosaugos leidimų informacinė sistema, Intelektuali miškų ūkio elektroninių paslaugų informacinė sistema, Saugomų rūšių informacinė sistema (toliau – informacinės sistemos).

2. Šios taisyklės yra parengtos vadovaujantis:

2.1. Bendraisiais elektroninės informacijos saugos valstybės institucijų ir įstaigų informacinėse sistemose reikalavimais, patvirtintais Lietuvos Respublikos Vyriausybės 1997 m. rugsėjo 4 d. nutarimu Nr. 952 (Žin., 1997, Nr. 83-2075; 2007, Nr. 49-1891);

2.2. Saugos dokumentų turinio gairėmis, patvirtintomis Lietuvos Respublikos vidaus reikalų ministro 2007 m. gegužės 8 d. įsakymu Nr. IV-172 (Žin., 2007, Nr. 53-2070);

2.3. Lietuvos Respublikos aplinkos ministerijos informacinių sistemų duomenų saugos nuostatais, patvirtintais Lietuvos Respublikos aplinkos ministro 2011 m. d. įsakymu Nr. .

3. Šiose taisyklėse vartojamos sąvokos apibrėžtos Lietuvos Respublikos aplinkos ministerijos informacinių sistemų duomenų saugos nuostatuose ir kituose teisės aktuose.

4. Ministerijos informacinėse sistemose esanti elektroninė informacija skirstoma į:

4.1. viešąją informaciją;

4.2. tarnybinio naudojimo informaciją.

II. TECHNINIŲ IR KITŲ SAUGOS PRIEMONIŲ APRAŠYMAS

5. Naudotojų prieiga prie informacinių sistemų išteklių turi būti valdoma naudotojų prieigos valdymo sistema.

6. Naudotojų kompiuterių apsaugai turi būti taikoma programinė įranga, efektyviai apsauganti nuo kenksmingo kodo programų (antivirusinė programinė įranga, nepageidaujamo turinio valdymo įranga ir pan.). Antivirusinės programinės įrangos kenksmingo kodo aprašai atnaujinami ne rečiau kaip kartą per dieną, naudojant centralizuotą apsaugos nuo kenksmingo kodo programų įrangą. Naudotojams apribota galimybė savavališkai keisti antivirusinės programinės įrangos nustatymus.

7. Naudotojų darbo vietos turi būti prijungiamos prie atskiros elektros energijos tiekimo tinklo atšakos.

8. Turi būti taikomos šios sisteminės ir taikomosios programinės įrangos apsaugos priemonės:

8.1. naudojama legali sisteminė ir taikomoji programinė įranga;

8.2. teisę dirbti su informacinėmis sistemomis, atliekant paslaugų administravimo funkcijas, turi informacinių sistemų administratorius;

8.3. slaptažodžius, suteikiančius teisę dirbti su informacinių sistemų tarnybinėmis stotimis ir jų administravimo programine įranga, žino tik administratorius;

8.4. informacinių sistemų duomenys techninėmis, organizacinėmis, programinėmis priemonėmis apsaugomi nuo praradimo, iškraipymo, sunaikinimo, neteisėto panaudojimo;

8.5. taikomos programinės priemonės Naudotojų tapatybei, jų veiksmams su informacinėmis sistemomis nustatyti.

9. Turi būti taikomos duomenų perdavimo tinklais apsaugos užtikrinimo priemonės:

9.1. Naudotojų kompiuterių apsaugai taikomos vietinės programinės ugniasienės. Įdiegiant vietines ugniasienes laikomasi principo „draudžiama viskas, išskyrus“, t.y. Naudotojui leidžiamas tik būtinas darbui duomenų perdavimo tinklo srautas. Vietinių ugniasienių sąranka valdoma centralizuotai.

9.2. Ministerijos duomenų perdavimo tinklas atskirtas nuo viešųjų telekomunikacijų tinklų ugniasiene.

9.3. už duomenų perdavimo tinklo ugniasienių priežiūrą, ugniasienės valdymo sistemos priežiūrą ir tinkamą ugniasienių sąranką yra atsakingas administratorius.

10. Patalpoms, kuriose veikia informacinių sistemų tarnybinės storys, turi būti taikomos patalpų ir aplinkos saugumo užtikrinimo priemonės:

10.1. patekimas į patalpą yra registruojamas žurnale, kuriame nurodomas asmens vardas, pavardė, asmens dokumento tipas ir numeris, darbovietė, patekimo tikslas ir pagrindas, sutarties, kurios pagrindu atliekami darbai, data ir numeris, patekimo laikas, išėjimo laikas;

10.2. patekimas į patalpas kontroliuojamas įeigos kontrolės priemonėmis;

10.3. leidimą patekti į patalpas duoda Ministerijos Informacinių technologijų skyriaus vedėjas;

10.4. pašalinių asmenų patekimas į patalpas leidžiamas tik dalyvaujant Ministerijos Informacinių technologijų skyriaus darbuotojui;

10.5. patalpose yra įdiegtos judesio ir gaisro signalizacijos.

11. Turi būti taikomos šios informacinių sistemų darbo apskaitos ir kitos elektroninės informacijos saugos užtikrinimo priemonės:

11.1. registruojami ir saugomi duomenys apie sistemos įjungimą, išjungimą, sėkmingus ir nesėkmingus bandymus registruotis sistemose, kitus saugai svarbius įvykius su nuoroda į naudotojo identifikatorių ir įvykio laiką;

11.2. Naudotojų kompiuterizuotose darbo vietose leidžiama naudoti tik su tarnybine veikla susijusią programinę įrangą. Kompiuterių vartotojų paskyros suteikia apribotas teises, kurios neleidžia įdiegti papildomos programinės įrangos;

11.3. Naudotojas be objektyvių priežasčių (kompiuteriu dirba keli asmenys ir pan.) negali leisti kitiems asmenims naudotis jiems darbo vietoje priskirta kompiuterine įranga;

11.4. Naudotojams draudžiama išsinešti Ministerijai priklausančią kompiuterių įrangą (stacionarius ir nešiojamuosius kompiuterius, spausdintuvus ir kt.), prieš tai nesuderinus su tiesioginiu vadovu.

IV. SAUGUS ELEKTRONINĖS INFORMACIJOS TVARKYMAS

12. Įvesti, keisti ir atnaujinti informacinių sistemų duomenis gali tik autorizuoti Naudotojai.

13. Informacinė sistema registruoja duomenų pakeitimus atlikusius informacinių sistemų Naudotojus ir duomenų keitimo laiką.

14. Duomenys apie Naudotojo veiksmus informacinėse sistemose turi būti saugomi registruojančios programinės įrangos gamintojų numatytą laiką.

15. Už atsarginių duomenų kopijų darymą, saugojimą ir duomenų atkūrimą iš atsarginių duomenų kopijų atsakingas Aplinkos ministerijos Informacinių technologijų skyrius:

15.1. kiekvieną naktį daro duomenų, esančių tarnybinėse stotyse, kopijas. Tai žymima žurnale;

15.2. atsižvelgiant į duomenų kiekį, jų atkūrimo laiką, duomenų laikmenų (kietieji diskai, magnetinės juostos ir pan.) talpą ir kiekį, duomenys gali būti archyvuojami visiškai (pilno archyvavimo tipas) arba iš dalies (inkrementinio ar diferencinio archyvavimo tipas);

15.3. Aplinkos ministerijos Informacinių technologijų skyrius, ir/arba įmonė su kuria sudaryta priežiūros sutartis, periodiškai, bet ne rečiau kaip kartą per metus, atlieka duomenų atkūrimą iš

atsarginių duomenų kopijų bandymus, siekiant įsitikinti, kad avarijos atveju atsarginių duomenų kopijomis galima pasikliauti;

15.4. rezervinės duomenų laikmenos saugomos atskiroje, pakankamai nutolusioje vietoje, kad, visiškai ar iš dalies praradus duomenis pagrindinėse patalpose dėl neigiamo aplinkos poveikio (gaisro, patalpų užliejimo, netinkamos aplinkos temperatūros techninei įrangai funkcionuoti ir pan.), jos nenukentėtų.

16. Duomenys perkeliami ir teikiami kitoms informacinėms sistemoms ir registrams, duomenys iš jų gaunami vadovaujantis Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymu bei duomenų teikimo sutartimis.

17. Sutartyse su trečiosiomis šalimis, susijusiomis su Ministerijos informacijos ar informacijos apdorojimo priemonių prieiga, duomenų apdorojimu, perdavimu ar valdymu turi būti numatytas reikalavimas pasirašyti konfidencialumo susitarimą.

18. Kopijuoti duomenis leidžiama tik veiklos tęstinumui užtikrinti.

19. Draudžiama kopijuoti, keisti, naikinti ar perduoti duomenis asmeniniais tikslais ar kitoms su tiesioginėmis pareigomis nesuderinamoms funkcijoms atlikti.

20. Operacinių sistemų, taikomosios programinės ir techninės įrangos keitimų ir naujinimų valdymas:

20.1. esminiai keitimai ir naujinimai identifikuojami ir registruojami;

20.2. keitimai ir naujinimai planuojami ir testuojami;

20.3. įvertinama su keitimų ir naujinimų poveikiu susijusi rizika, įskaitant poveikį saugumui;

20.4. numatyta formali keitimų ir naujinimų tvirtinimo procedūra;

20.5. su informacija apie keitimus supažindinamos visos susijusios šalys (naudotojai, administratoriai, saugos įgaliotinis ir kt.);

20.6. numatomos atstatomosios/grįžtamosios procedūros nesėkmingų keitimų ar naujinimų atvejams.

V. REIKALAVIMAI PASLAUGOMS IR JŲ TEIKĖJAMS

21. Paslaugų teikėjų prieigos prie informacinių sistemų lygiai ir sąlygos:

21.1. paslaugų teikėjams suteikiama tiktai tokia prieiga prie informacinių sistemų, kuri būtina sutartyse numatytiems įsipareigojimams vykdyti;

21.2. trečiųjų šalių loginė prieiga prie Ministerijos informacijos ir fizinis patekimas į patalpas turi būti saugomi organizacinėmis ir techninėmis priemonėmis:

21.2.1. paslaugų teikėjų patekimas į patalpas galimas tik lydint atsakingam darbuotojui;

21.2.2. visi paslaugų teikėjų veiksmai su informacinių sistemų duomenimis yra fiksuojami;

21.2.3. pasibaigus sutartyje nurodytam laikotarpiui, administratorius panaikina paslaugų teikėjo prieigos prie informacinių sistemų teisę.

22. Reikalavimai informacinių sistemų paslaugų tiekėjų teikiamoms paslaugoms:

22.1. reikalavimai paslaugų teikėjams ir jų teikiamoms paslaugoms nustatomi šių paslaugų teikimo sutartyse;

22.2. su trečiosiomis šalimis sudarytose sutartyse, kurios susijusios su informacinių sistemų informacijos ar informacijos apdorojimo priemonių prieiga, duomenų apdorojimu, perdavimu ar valdymu, turi būti numatytas reikalavimas pasirašyti konfidencialumo susitarimą;

22.3. paslaugų teikėjas įsipareigoja laikytis šiame ir susijusiuose dokumentuose numatytų saugumo reikalavimų;

22.4. jei rangovas darbams atlikti arba paslaugoms teikti samdo subrangovus, Ministerijos ir rangovo sutartyje apibrėžti saugumo reikalavimai turi būti taikomi ir subrangovui ir turi būti įtraukti į rangovo ir subrangovo sutartį.

VII. BAIGIAMOSIOS NUOSTATOS

23. Šios Taisyklės yra privalomos visiems Naudotojams.
24. Naudotojai, pažeidę šias Taisykles, atsako teisės aktų nustatyta tvarka.

_____