PATVIRTINTA
Lietuvos Respublikos aplinkos ministro
2012 m. liepos 25 d. įsakymu Nr.D1-637
(Lietuvos Respublikos aplinkos ministro
2016 m. vasario 19 d. įsakymo Nr. D1-
123 redakcija)

LIETUVOS RESPUBLIKOS APLINKOS MINISTERIJOS INFORMACINIŲ SISTEMŲ SAUGAUS ELEKTRONINĖS INFORMACIJOS TVARKYMO TAISYKLĖS

I. BENDROSIOS NUOSTATOS

1. Lietuvos Respublikos aplinkos ministerijos (toliau – Ministerija) informacinių sistemų (toliau – Informacinės sistemos) saugaus elektroninės informacijos tvarkymo taisyklės (toliau – Taisyklės) nustato tvarką, užtikrinančią saugų Ministerijos informacinių sistemų (toliau – Informacinės sistemos), nurodytų Informacinių sistemų duomenų saugos nuostatuose (toliau – Saugos nuostatai), elektroninės informacijos tvarkymą, technines ir kitas Informacinių sistemų saugos priemones, Informacinių sistemų funkcionavimui reikalingoms paslaugoms ir jų teikėjams keliamus reikalavimus.

2. Taisyklėse vartojamos sąvokos apibrėžtos Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatyme, Bendrųjų elektroninės informacijos saugos reikalavimų apraše, patvirtintame Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašo patvirtinimo“.

3. Visa tvarkoma elektroninė informacija yra nurodyta atitinkamos Informacinės sistemos nuostatuose ir priskiriama žinybinės svarbos informacijos kategorijai.

4. Už Informacinių sistemų elektroninės informacijos tvarkymą atsakingi Naudotojai, kuriems tokia teisė yra suteikta. Teises suteikia ir prižiūri Informacinių sistemų administratoriai.

II. TECHNINIŲ IR KITŲ SAUGOS PRIEMONIŲ APRAŠYMAS

5. Kompiuterinės įrangos saugos priemonės:

5.1. visa Informacinių sistemų tarnybinių stočių įranga privalo turėti šios įrangos gamintojų garantinį arba pratęstą pogarantinį aptarnavimą;

5.2. Informacinės sistemos tarnybinių stočių įranga turi perspėti Administratorių, kai tarnybinėse stotyse sumažėja iki nustatytos ribos laisvos operatyviosios atminties ar vietos diskuose ar duomenų saugykloje, ilgą laiką stipriai apkraunamas centrinis procesorius ir/ar tinklo sąsaja;

5.3. techninė įranga turi rezervinį maitinimo šaltinį su įtampos filtrais, kurie užtikrina nepertraukiamą Informacinių sistemų pagrindinės kompiuterinės įrangos veikimą;

5.4. Informacinių sistemų Naudotojų kompiuterinėje įrangoje naudojama tik legali ir darbo funkcijoms atlikti reikalinga programinė įranga. Informacinės sistemos saugos įgaliotinis parengia, su Informacinės sistemos valdytojo vadovu suderina ir ne rečiau kaip kartą per metus peržiūri bei prireikus atnaujina leistinos programinės įrangos sąrašą;

5.5. Informacinių sistemų prieinamumas per metus užtikrinamas ne mažiau kaip 90 proc. laiko darbo metu darbo dienomis;

5.6. Informacinių sistemų programinė įranga apsaugota nuo pagrindinių per tinklą vykdomų atakų;

5.7. Informacinių sistemų taikomoji programinė įranga testuojama naudojant atskirą testavimui skirtą aplinką nenaudojant asmens duomenų. Tais atvejais, kai asmens duomenys yra būtini testavimams, asmens duomenys naudojami vadovaujantis Bendrųjų reikalavimų organizacinėms ir

techninėms duomenų saugumo priemonėms, patvirtintų Valstybinės duomenų apsaugos inspekcijos direktoriaus 2008 m. lapkričio 12 d. įsakymu Nr. 1T-71(1.12), 10.10 punkto reikalavimais.

6. Sisteminės ir taikomosios įrangos saugos priemonės:

6.1. naudojama legali sisteminė ir taikomoji programinė įranga;

6.2. teisę dirbti su Informacinėmis sistemomis, atliekant administravimo funkcijas, turi tik Administratoriai;

6.3. slaptažodžius, suteikiančius teisę dirbti su Informacinės sistemos tarnybinėmis stotimis ir jų administravimo programine įranga, žino tik Administratorius;

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

6.5. taikomos programinės priemonės Naudotojų tapatybei, jų veiksmams su Informacinėmis sistemomis nustatyti.

7. Elektroninės informacijos perdavimo tinklais saugumo užtikrinimo priemonės:

7.1. 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;

7.2. Ministerijos duomenų perdavimo tinklas atskirtas nuo viešųjų telekomunikacijų tinklų ugniasiene;

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

7.4. nuotolinis prisijungimas prie Informacinių sistemų vykdomas protokolu, skirtu duomenų šifravimui.

8. Patalpų ir aplinkos saugumo užtikrinimo priemonės:

8.1. 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;

8.2. patekimas į patalpas kontroliuojamas įeigos kontrolės priemonėmis;

8.3. leidimą patekti į patalpas duoda Ministerijos Informacinių technologijų skyriaus vedėjas, o, jei jo nėra, – jį pavaduojantis asmuo;

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

8.5. patalpose yra įdiegtos judesio signalizacijos, įrengti įsilaužimo davikliai, prijungti prie pastato signalizacijos ir apsaugos tarnybos stebėjimo pulto;

8.6. patalpos atitinka priešgaisrinės saugos reikalavimus, jose yra gaisro gesinimo priemonės, įrengti gaisro davikliai, prijungti prie pastato signalizacijos ir apsaugos tarnybos stebėjimo pulto;

8.7. patalpose įrengta kondicionavimo sistema, palaikoma + 22 (± 5) °C temperatūra ir 50 (± 10) procentų santykinis oro drėgnumas;

9. Kitos priemonės, naudojamos elektroninės informacijos saugai užtikrinti:

9.1. 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;

9.2. 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;

9.3. Naudotojų kompiuterių apsaugai turi būti taikoma programinė įranga, efektyviai apsauganti nuo kenksmingo kodo programų (antivirusinė programinė įranga, nepageidaujamo turinio valdymo įranga ir pan.). Naudotojams apribota galimybė savavališkai keisti antivirusinės programinės įrangos nustatymus;

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

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

9.6. Informacinių sistemų neveikimo laikotarpis negali būti ilgesnis nei 16 val.;

9.7. Informacinių sistemų informacinių technologijų saugos atitikties vertinimas atliekamas ne rečiau kaip kartą per dvejus metus.

III. SAUGUS ELEKTRONINĖS INFORMACIJOS TVARKYMAS

10. Įvesti, keisti ir atnaujinti Informacinių sistemų duomenis gali tik tam teisę turintys autorizuoti Naudotojai.

11. Informacinė sistema registruoja duomenų pakeitimus atlikusius Naudotojus ir duomenų keitimo laiką.

12. Kopijuoti duomenis leidžiama tik Informacinių sistemų veiklos tęstinumui užtikrinti.

13. 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.

14. Kopijuoti, keisti, naikinti ar perduoti duomenis asmeniniais tikslais ar kitoms su tiesioginėmis pareigomis nesuderinamoms funkcijoms atlikti griežtai draudžiama.

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 (visiško 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 atkūrimo 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. Informacinių sistemų taikomoji programinė įranga turi įvestos elektroninės informacijos tikslumo, užbaigtumo ir patikimumo tikrinimo priemones.

17. Informacinių sistemų programinės ir techninės įrangos keitimo ir atnaujinimo tvarka:

17.1. esminiai keitimai identifikuojami ir registruojami;

17.2. keitimai planuojami ir testuojami tam skirtoje testavimo aplinkoje;

17.3. įvertinama su keitimų poveikiu susijusi rizika, įskaitant poveikį saugumui;

17.4. su informacija apie keitimus supažindinamos visos su Informacinių sistemų veikla susijusios šalys (Naudotojai, Administratorius, Saugos įgaliotiniai ir kt.);

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

18. Informacinių sistemų pokyčių (toliau – pokyčiai) valdymo tvarka, apimanti šiuos procesus:

18.1. pokyčių identifikavimas;

18.2. pokyčių suskirstymas į kategorijas, atsižvelgiant į pokyčių svarbą, aktualumą, poreikį ir panašiai;

18.3. pokyčių įtakos vertinimas;

18.4. pokyčių prioritetų nustatymas;

18.5. pokyčių atlikimas.

19. Elektroninės informacijos neteisėto kopijavimo, keitimo, naikinimo ar perdavimo nustatymo tvarka:

19.1. siekiant užtikrinti Informacinių sistemų duomenų vientisumą, Naudotojų tapatybei nustatyti ir prieigai kontroliuoti naudojama prisijungimo vardų, slaptažodžių ir teisių sistema;

19.2. Naudotojas, įtaręs, kad su Informacinės sistemos duomenimis buvo atlikti neteisėti veiksmai, privalo pranešti apie tai Informacinės sistemos administratoriui. Informacinės sistemos administratorius, atsiradus įtarimams dėl neteisėtų veiksmų su Informacinės sistemos duomenimis, pasinaudojęs Informacinės sistemos veiksmų žurnalo įrašais, nustato neteisėto poveikio šaltinį, laiką ir veiksmus, atliktus su Informacinės sistemos programine įranga ir (ar) duomenimis;

19.3. Administratorius, įtaręs, kad su Informacinės sistemos duomenimis vykdomi neteisėti veiksmai, privalo apie tai pranešti Informacinės sistemos saugos įgaliotiniui;

19.4. Saugos įgaliotinis, gavęs pranešimą apie vykdomus neteisėtus veiksmus su Informacine sistema arba su Informacinėje sistemoje tvarkomais duomenimis, inicijuoja elektroninės informacijos saugos incidento valdymo procedūras;

19.5. apie pastebėtus saugos incidentus – Taisyklių reikalavimų pažeidimus, Informacinės sistemos darbo sutrikimus, neįprastą Informacinės sistemos veikimą – Naudotojas privalo informuoti Informacinės sistemos saugos įgaliotinį.

20. Nešiojamųjų kompiuterių ir kitų mobiliųjų įrenginių naudojimo tvarka:

20.1. nešiojamiesiems kompiuteriams, kuriems suteikiama prieiga prie vidinio tinklo bei jų naudotojams taikomi visi stacionarioms kompiuterizuotoms darbo vietoms ir jų naudotojams numatyti saugumo reikalavimai;

20.2. nuotolinis prisijungimas prie vidinio tinklo nėra leistinas, išskyrus:

20.2.1. Ministerijos viešai teikiamas paslaugas;

20.2.2. Ministerijos Informacinių technologijų skyriaus darbuotojus sistemų administravimui;

20.2.3. kai yra gautas Ministerijos Informacinių technologijų skyriaus leidimas.

IV. REIKALAVIMAI, KELIAMI INFORMACINĖMS SISTEMOMS FUNKCIONUOTI REIKALINGOMS PASLAUGOMS IR JŲ TEIKĖJAMS

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

21.1. paslaugų teikėjams suteikiama tik 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 Informacinės sistemos teises.

22. Reikalavimai Informacinių sistemų paslaugų teikėjų 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.

_____