LIETUVOS POLICIJOS GENERALINIO KOMISARO
Į S A K Y M A S

DĖL LIETUVOS POLICIJOS GENERALINIO KOMISARO 2008 M. SAUSIO 8 D. ĮSAKYMO NR. 5-V-8 „DĖL POLICIJOS ŽINYBINIŲ REGISTRŲ IR POLICIJOS ELEKTRONINIŲ PASLAUGŲ SISTEMOS DUOMENŲ SAUGOS NUOSTATŲ PATVIRTINIMO“ PAKEITIMO

2011 m. balandžio 18 d. Nr. 5-V-340
Vilnius

Vadovaudamasis Bendrųjų elektroninės informacijos saugos valstybės institucijų ir įstaigų informacinėse sistemose reikalavimų, patvirtintų Lietuvos Respublikos Vyriausybės 1997 m. rugsėjo 4 d. nutarimu Nr. 952 „Dėl elektroninės informacijos saugos valstybės institucijų ir įstaigų informacinėse sistemose“ (Žin., 1997, Nr. 83-2075; 2007, Nr. 49-1891), 6.1 punktu:

1. P a k e i č i u Policijos žinybinių registrų ir policijos elektroninių paslaugų sistemos duomenų saugos nuostatus, patvirtintus Lietuvos policijos generalinio komisaro 2008 m. sausio 8 d. įsakymu Nr. 5-V-8 „Dėl Policijos žinybinių registrų ir policijos elektroninių paslaugų sistemos duomenų saugos nuostatų patvirtinimo“ (kartu su 2010 m. balandžio 28 d. įsakymu Nr. 5-V-342), ir išdėstau juos nauja redakcija (pridedama).

2. P r i p a ž į s t u netekusiu galios Lietuvos policijos generalinio komisaro 2006 m. liepos 28 d. įsakymo Nr. 5-V-468 „Dėl Policijos informacinės sistemos personalo posistemio steigimo ir jo nuostatų patvirtinimo“ 2.2 punktą.

3. S k e l b i u šį įsakymą Policijos departamento prie Vidaus reikalų ministerijos interneto svetainėje.

POLICIJOS GENERALINIS KOMISARAS SAULIUS SKVERNELIS

SUDERINTA
Informatikos ir ryšių departamento prie
Lietuvos Respublikos vidaus reikalų ministerijos
2011 m. balandžio 5 d. raštu Nr.(6-7) 9R-4005

PATVIRTINTA
Lietuvos policijos generalinio komisaro
2008 m. sausio 8 d. įsakymu Nr. 5-V-8
(Lietuvos policijos generalinio komisaro
2011 m. balandžio 18 d.
įsakymo Nr.5-V-340 redakcija)

POLICIJOS INFORMACINĖS SISTEMOS DUOMENŲ SAUGOS NUOSTATAI

I. BENDROSIOS NUOSTATOS

1. Policijos informacinės sistemos duomenų saugos nuostatai (toliau – Saugos nuostatai) nustato principus ir reikalavimus, užtikrinančius saugų policijos žinybinių registrų, posistemių ir kitų informacinių sistemų (toliau – POLIS) (POLIS sudėtinių dalių), elektroninės informacijos tvarkymą, reglamentuoja POLIS saugos politiką.

2. Saugos nuostatai parengti vadovaujantis Bendraisiais elektroninės informacijos saugos valstybės institucijų ir įstaigų informacinėse sistemose reikalavimais, patvirtintais Lietuvos Respublikos Vyriausybės 1997 m. rugsėjo 4 d. nutarimu Nr. 952 „Dėl elektroninės informacijos saugos valstybės institucijų ir įstaigų informacinėse sistemose“ (Žin., 1997, Nr. 83-2075; 2007, Nr. 49-1891) (toliau – Saugos reikalavimai), Saugos dokumentų turinio gairėmis, patvirtintomis Lietuvos Respublikos vidaus reikalų ministro 2007 m. gegužės 8 d. įsakymu Nr. 1V-172 (Žin., 2007, Nr. 53-2070) (toliau – Saugos dokumentų turinio gairės), Valstybės institucijų ir įstaigų informacinių sistemų klasifikavimo pagal jose tvarkomą elektroninę informaciją gairėmis, patvirtintomis Lietuvos Respublikos vidaus reikalų ministro 2007 m. liepos 11 d. įsakymu Nr. 1V-247 (Žin., 2007, Nr. 78-3160) (toliau – Informacinių sistemų klasifikavimo gairės), Valstybės institucijų ir įstaigų informacinių sistemų elektroninės informacijos techniniais saugos reikalavimais, patvirtintais Lietuvos Respublikos vidaus reikalų ministro 2008 m. spalio 27 d. įsakymu Nr. 1V-384 (Žin., 2008, Nr. 127-4866) (toliau – Informacinių sistemų elektroninės informacijos techniniai saugos reikalavimai), ir kitais teisės aktais bei Lietuvos standartais LST ISO/IEC 27001:2006 ir LST ISO/IEC 27002:2009. Šiuose Saugos nuostatuose vartojamos sąvokos atitinka išvardytuose teisės aktuose vartojamas sąvokas.

3. Saugos nuostatų reikalavimai taikomi tvarkant:

3.1. Policijos registruojamų įvykių registrą;

3.2. Administracinių teisės pažeidimų ir eismo įvykių registrą;

3.3. Ieškomų ginklų registrą;

3.4. Ieškomų transporto priemonių registrą;

3.5. Ieškomų ir rastų numeruotų bei individualius požymius turinčių daiktų ir dokumentų registrą;

3.6. Prevencinių poveikio priemonių taikymo registrą;

3.7. Daktiloskopinių duomenų registrą;

3.8. DNR duomenų registrą;

3.9. Civilinėje apyvartoje esančių ginklų registrą;

3.10. policijos elektroninių paslaugų sistemą;

3.11. personalo posistemį;

3.12. dokumentų registracijos posistemį;

3.13. mokymų organizavimo posistemį;

3.14. tinklo ir kompiuterizuotų darbo vietų apskaitos posistemį;

3.15. buhalterinės apskaitos ir biudžeto posistemį;

3.16. policijos tarnybinio elektroninio pašto sistemą;

3.17. naudotojų administravimo sistemą;

3.18. Vieningą pajėgų valdymo sistemą.

4. Elektroninės informacijos saugumo tikslai:

4.1. sudaryti sąlygas saugiai automatiniu būdu tvarkyti elektroninę informaciją POLIS;

4.2. užtikrinti, kad elektroninė informacija būtų patikima ir apsaugota nuo atsitiktinio ar neteisėto sunaikinimo, pakeitimo, atskleidimo, kitokio neteisėto jos tvarkymo.

5. Elektroninės informacijos saugumo užtikrinimo prioritetinės kryptys:

5.1. elektroninės informacijos konfidencialumo, vientisumo ir prieinamumo užtikrinimas;

5.2. veiklos tęstinumas;

5.3. POLIS naudotojų mokymas;

5.4. asmens duomenų apsauga.

6. Saugos nuostatai taikomi POLIS valdytojui ir registrų tvarkymo įstaigoms (toliau – tvarkytojams).

7. POLIS valdytojo ir tvarkytojų pavadinimai ir adresai:

7.1. POLIS valdytojas yra Policijos departamentas prie Vidaus reikalų ministerijos (toliau – Policijos departamentas). Buveinės adresas – Saltoniškių g. 19, LT-08105 Vilnius;

7.2. POLIS tvarkytojai:

7.2.1. teritorinės, specializuotos policijos ir policijos profesinio mokymo įstaigos. POLIS tvarkymo įstaigų buveinių adresai pateikiami Policijos departamento tinklalapyje adresu http://www.policija.lt/, skiltyje „Struktūra ir kontaktai“;

7.2.2. kitos institucijos, kurioms POLIS valdytojas teisės aktų nustatyta tvarka suteikė įgaliojimus tvarkyti POLIS duomenis.

8. Policijos departamento, kaip POLIS valdytojo, funkcijos ir atsakomybė:

8.1. priimti sprendimus dėl POLIS informacinių technologijų atitikties Saugos reikalavimams vertinimo atlikimo;

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

8.3. skirti POLIS saugos įgaliotinį;

8.4. rengti POLIS kūrimo, plėtros ir panaikinimo planus;

8.5. prižiūrėti POLIS kūrimą, diegimą ir tvarkymą;

8.6. atlikti kitas Saugos nuostatų, Saugos reikalavimų, žinybinių registrų, posistemių ir kitų informacinių sistemų nuostatų ir kitų teisės aktų nustatytas funkcijas.

9. POLIS tvarkytojų funkcijos ir atsakomybė:

9.1. tvarkyti POLIS duomenis įstatymų, Saugos nuostatų ir kitų teisės aktų nustatyta tvarka;

9.2. užtikrinti POLIS duomenų saugą;

9.3. teikti siūlymus POLIS valdytojui dėl techninių, programinių priemonių, skirtų POLIS eksploatuoti ir prižiūrėti, įsigijimo ir atnaujinimo;

9.4. atlikti kitas Saugos nuostatų, Saugos reikalavimų, žinybinių registrų, posistemių ir informacinių sistemų nuostatų, duomenų teikimo sutarčių ir kitų teisės aktų nustatytas funkcijas.

10. Informatikos ir ryšių departamentas prie Lietuvos Respublikos vidaus reiklų ministerijos atlieka policijos žinybinių registrų nuostatų ir kitų teisės aktų nustatytas saugos funkcijas.

11. Saugos įgaliotinio, įgyvendinančio elektroninės informacijos saugą POLIS, funkcijos ir atsakomybė:

11.1. teikti POLIS valdytojui siūlymus dėl:

11.1.1. administratorių, kuriuos turi teisę skirti POLIS valdytojas, skyrimo (saugos įgaliotinis negali atlikti POLIS administratoriaus funkcijų);

11.1.2. saugos politiką įgyvendinančių dokumentų priėmimo, keitimo ar panaikinimo;

11.1.3. POLIS atitikties Saugos reikalavimams vertinimo atlikimo;

11.2. koordinuoti elektroninės informacijos saugos incidentų, įvykusių POLIS, tyrimą (išskyrus atvejus, kai šią funkciją atlieka veiklos tęstinumo valdymo grupė);

11.3. teikti administratoriams privalomus vykdyti nurodymus ir pavedimus;

11.4. atlikti kitas POLIS valdytojo vadovo pavestas funkcijas.

12. Administratoriaus, vykdančio POLIS priežiūrą, funkcijos ir atsakomybė:

12.1. vertinti POLIS naudotojų pasirengimą dirbti su POLIS;

12.2. suteikti, keisti ir panaikinti prieigos prie POLIS teises;

12.3. rengti ir tikrinti (peržiūrėti) POLIS sudarančių komponentų sąranką;

12.4. atlikti POLIS pažeidžiamų vietų nustatymą;

12.5. pagal kompetenciją atlikti POLIS taikomų saugumo reikalavimų atitikties vertinimą;

12.6. informuoti saugos įgaliotinį apie saugos dokumentų pažeidimus, nusikalstamos veikos požymius, neveikiančias arba netinkamai veikiančias duomenų saugos užtikrinimo priemones;

12.7. atlikti kitas POLIS valdytojo vadovo ar saugos įgaliotinio pavestas funkcijas, pvz., atsakyti už POLIS funkcionavimą užtikrinančios techninės ir programinės įrangos, infrastruktūros bei informacinių technologijų paslaugų administravimą, vardų skyrimą, atsakyti už priskirtų POLIS komponentų (kompiuterizuotų darbo vietų (toliau – KDV), tarnybinių stočių, operacinių sistemų, duomenų bazių, užkardų, įsilaužimo aptikimo sistemų, duomenų perdavimo tinklų) administravimą, POLIS komponentų sąrankos aprašymo dokumentacijos parengimą ir atnaujinimą, saugos priemonių POLIS pažeidžiamoms vietoms parinkimą bei jų atitiktį saugos politikos (išdėstytos Saugos nuostatuose) ir saugos politiką įgyvendinančių dokumentų (Saugaus policijos informacinės sistemos žinybinių registrų ir posistemių elektroninės informacijos tvarkymo taisyklės (Lietuvos policijos generalinio komisaro 2008 m. spalio 2 d. įsakymas Nr. 5-V-584), POLIS veiklos tęstinumo valdymo planu (Lietuvos policijos generalinio komisaro 2011 m. balandžio 14 d. įsakymas Nr. 5-V-335) ir Naudotojų, dirbančių su registrais ir informacinėmis sistemomis, administravimo taisyklėmis (Lietuvos policijos generalinio komisaro 2008 m. gruodžio 16 d. įsakymas Nr. 5-V-775)) reikalavimams, pagal kompetenciją rengti pasiūlymus dėl POLIS palaikymo, priežiūros, techninės ir programinės įrangos modernizavimo ir elektroninės informacijos saugos užtikrinimo, registruoti elektroninės informacijos saugos incidentus ir informuoti apie juos saugos įgaliotinį, teikti siūlymus dėl minėtų incidentų pašalinimo, užtikrinti POLIS duomenų konfidencialumą, vientisumą ir prieinamumą, atlikti kitas Saugos nuostatuose ir kituose saugos politiką įgyvendinančiuose dokumentuose nustatytas funkcijas.

13. POLIS naudotojai:

13.1. vadovaudamiesi POLIS valdytojo patvirtintais žinybinių registrų, posistemių ir informacinių sistemų nuostatais, šiais Saugos nuostatais, Naudotojų, dirbančių su registrais ir informacinėmis sistemomis, administravimo taisyklėmis, Saugaus policijos informacinės sistemos žinybinių registrų ir posistemių elektroninės informacijos tvarkymo taisyklėmis ir pareigybių aprašymais, naudojasi POLIS;

13.2. užtikrina duomenų tvarkymo teisėtumą;

13.3. informuoja saugos įgaliotinį, administratorių apie elektroninės informacijos saugos incidentus, POLIS darbo sutrikimus;

13.4. vykdo kitas šiuose Saugos nuostatuose ir saugos politiką įgyvendinančiuose dokumentuose nustatytas funkcijas ir kitus POLIS valdytojo, saugos įgaliotinio ir administratoriaus nurodymus, susijusius su POLIS naudojimu ir sauga.

14. Teisės aktai, kuriais vadovaujantis tvarkomi POLIS duomenys ir užtikrinama jų sauga:

14.1. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas (Žin., 1996, Nr. 63-1479; 2008, Nr. 22-804);

14.2. Lietuvos Respublikos valstybės registrų įstatymas (Žin., 1996, Nr. 86-2043; 2004, Nr. 124-4488);

14.3. Saugos reikalavimai;

14.4. Saugos dokumentų turinio gairės;

14.5. Informacinių sistemų klasifikavimo gairės;

14.6. Informacinių sistemų elektroninės informacijos techniniai saugos reikalavimai;

14.7. Lietuvos standartai LST ISO/IEC 27001:2006 „Informacijos technologija. Saugumo metodai. Informacijos saugumo valdymo sistemos. Reikalavimai“, LST ISO/IEC 27002:2009 „Informacijos technologija. Saugumo metodai. Informacijos saugumo valdymo praktikos kodeksas“ ir kiti Lietuvos ir tarptautiniai „Informacijos technologija. Saugumo metodai“ grupės standartai, apibūdinantys saugų informacinės sistemos duomenų tvarkymą;

14.8. kiti teisės aktai, reglamentuojantys POLIS duomenų tvarkymo teisėtumą, POLIS tvarkytojų veiklą ir duomenų saugą.

II. ELEKTRONINĖS INFORMACIJOS SAUGOS VALDYMAS

15. Atsižvelgiant į POLIS duomenų savybių (vientisumo, konfidencialumo ir prieinamumo) įtaką policijos veiklai, POLIS sudėtinės dalys, išvardytos Saugos nuostatų 3 punkte, vadovaujantis Informacinių sistemų klasifikavimo gairėmis, yra priskiriamos:

15.1. POLIS sudėtinės dalys, nurodytos Saugos nuostatų 3.1–3.11 punktuose, – antrajai informacinių sistemų kategorijai;

15.2. POLIS sudėtinės dalys, nurodytos Saugos nuostatų 3.12–3.18 punktuose, – trečiajai informacinių sistemų kategorijai.

16. POLIS saugos priemonės parenkamos įvertinus galimus rizikos POLIS duomenų vientisumui, konfidencialumui ir prieinamumui veiksnius. Pasirenkant saugos priemones prioritetas teikiamas toms priemonėms, kurių diegimas duoda didžiausią poveikį ir reikalauja mažiausiai sąnaudų.

17. Saugos įgaliotinis, atsižvelgdamas į Vidaus reikalų ministerijos išleistą metodinę priemonę „Rizikos analizės vadovas“, Lietuvos ir tarptautinius „Informacijos technologija. Saugumo technika“ grupės standartus ir taikydamas pasaulyje pripažintas metodikas bei vadovaudamasis Galimų grėsmių ir rizikų Policijos informacinei sistemai analizavimo, stebėjimo ir vertinimo procedūrų aprašu, patvirtintu Lietuvos policijos generalinio komisaro 2010 m. birželio 3 d. įsakymu Nr. 5-V-456, kasmet atlieka POLIS rizikos vertinimą, o prireikus ir neeilinį rizikos vertinimą iki liepos 1 dienos. Prireikus POLIS valdytojo pavedimu POLIS rizikos vertinimui atlikti gali būti samdoma privati įmonė.

18. POLIS rizikos vertinimo rezultatai išdėstomi rizikos vertinimo ataskaitoje.

19. Rizikos veiksnių tikimybės ir žalos vertinimo klasifikacija:

19.1. maža rizikos veiksnių tikimybė, žala – 1 balas;

19.2. maža–vidutinė rizikos veiksnių tikimybė, žala – 2 balai;

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

19.4. vidutinė–didelė rizikos veiksnių tikimybė, žala – 4 balai;

19.5. didelė rizikos veiksnių tikimybė, žala – 5 balai.

20. Atsižvelgdamas į rizikos vertinimo ataskaitą, POLIS valdytojo vadovas prireikus tvirtina POLIS rizikos įvertinimo ir rizikos valdymo priemonių planą, kuriame numatomos rizikos mažinimo priemonės bei techninių, administracinių ir organizacinių išteklių poreikis šioms priemonėms įgyvendinti.

21. Siekiant užtikrinti saugos politikos ir ją įgyvendinančių teisės aktų nustatytų reikalavimų įgyvendinimo organizavimą ir kontrolę, ne rečiau kaip kartą per dvejus metus organizuojamas POLIS informacinių technologijų saugos atitikties vertinimas, kurio metu:

21.1. įvertinama Saugos nuostatų ir saugos politiką įgyvendinančių teisės aktų atitiktis realiai POLIS saugos situacijai;

21.2. inventorizuojama POLIS techninė ir programinė įranga;

21.3. patikrinama ne mažiau kaip 10 procentų atsitiktinai parinktų POLIS naudotojų KDV, visose tarnybinėse stotyse įdiegta programinė įranga ir jų sąranka;

21.4. patikrinama (įvertinama) POLIS naudotojams suteiktų teisių ir vykdomų funkcijų atitiktis;

21.5. įvertinamas pasirengimas užtikrinti POLIS veiklos tęstinumą įvykus elektroninės informacijos saugos incidentui.

22. Atlikus POLIS informacinių technologijų saugos atitikties vertinimą, rengiamas pastebėtų trūkumų šalinimo planas, kurį tvirtina, atsakingus vykdytojus paskiria ir įgyvendinimo terminus nustato POLIS valdytojo vadovas.

III. ORGANIZACINIAI IR TECHNINIAI REIKALAVIMAI

23. Priemonės ir metodai, kurie taikomi užtikrinant prieigą prie POLIS, nurodant leistiną šios prieigos laiką ir būdą, nustatomi Naudotojų, dirbančių su registrais ir informacinėmis sistemomis, administravimo taisyklėse.

24. Bendrosios priemonės ir metodai:

24.1. POLIS naudotojai jungiasi prie POLIS naudodami POLIS programinę įrangą bei technines ir kitas programines priemones, užtikrinančias saugų duomenų perdavimą;

24.2. POLIS naudotojai atpažįstami pagal unikalius POLIS naudotojų vardus ir slaptažodžius, kurių automatizuotą kontrolę atlieka KDV ir tarnybinių stočių operacinės sistemos. Teisės POLIS naudotojams naudotis POLIS suteikiamos vadovaujantis prašymu ir atsižvelgiant į vykdomas funkcijas;

24.3. prireikus (jei būtina POLIS veiklai užtikrinti) galimas administratoriaus prisijungimas prie KDV ir tarnybinių stočių operacinių sistemų valdymo ir konfigūravimo nuotoliniu būdu, naudojant virtualų privatų tinklą;

24.4. fiksuojami visi POLIS naudotojų, dirbančių su POLIS, duomenų tvarkymo veiksmai;

24.5. registruojami, sprendžiami ir šalinami POLIS naudotojų KDV incidentai;

24.6. kontroliuojamas patekimas į tarnybinių stočių patalpas, veikia signalizacija (nuo įsilaužimo ir gaisro);

24.7. ilgiausias neaktyvumo laikas, kuriam pasibaigus POLIS naudotojų ryšio sesijos yra automatiškai nutraukiamos, yra 30 minučių. POLIS naudotojų prieigos teisės yra blokuojamos, jei suteiktas prisijungimo vardas yra nenaudojamas 90 dienų;

24.8. POLIS prieinamumas užtikrinamas naudojant dviejų rūšių atsarginio maitinimo šaltinius (skirtus laikiniems elektros sutrikimams, kurie gali tęstis nuo 10 iki 30 min., išvengti) ir dyzelinį generatorių – ilgalaikiams elektros sutrikimams.

25. Programinės įrangos, skirtos POLIS ir KDV nuo kenksmingos programinės įrangos apsaugoti, naudojimo nuostatos:

25.1. visose POLIS tarnybinėse stotyse ir KDV, kuriose dirbama su POLIS duomenimis, privalo būti naudojama programinė įranga, skirta POLIS ir KDV nuo kenksmingos programinės įrangos apsaugoti;

25.2. POLIS duomenims ir KDV nuo kenksmingos programinės įrangos apsaugoti POLIS valdytojo ir tvarkytojų įstaigose turi būti naudojamos legalios programinės priemonės;

25.3. POLIS naudotojų kompiuteriuose naudojama įranga, skirta KDV nuo kenksmingos programinės įrangos apsaugoti, turi apsaugoti ir elektroninio pašto programinę įrangą nuo nepageidaujamo pašto ar kenksmingų programų patekimo į KDV;

25.4. POLIS naudotojų kompiuteriuose esanti programinė įranga, skirta POLIS ir KDV nuo kenksmingos programinės įrangos apsaugoti, turi būti atnaujinama automatiniu būdu ne rečiau kaip kas trys dienos;

25.5. atsiradus požymių, kad KDV yra kenksmingų programų, turi būti patikrinami visi KDV standieji diskai, naudojama programinė įranga, skirta POLIS ir KDV nuo kenksmingos programinės įrangos apsaugoti;

25.6. KDV esančios programinės įrangos, skirtos POLIS ir KDV nuo kenksmingos programinės įrangos apsaugoti, nustatymai turi būti parinkti pagal rekomenduojamus tokios programinės įrangos gamintojų reikalavimus arba pagal vidinio kompiuterių tinklo administratoriaus rekomendacijas;

25.7. POLIS programinis kodas privalo būti apsaugotas nuo atskleidimo neturintiems teisės su juo susipažinti asmenims.

26. Programinės įrangos naudojimo nuostatos:

26.1. POLIS naudotojams draudžiama diegti ir naudoti bet kokią programinę įrangą, keisti sistemos, kompiuterio ar programinės įrangos sistemų nustatymus. Programinę įrangą, reikalingą POLIS naudotojo funkcijoms atlikti, KDV diegia, atnaujina, kontroliuoja ir prižiūri tik administratorius. Kai diegimą turi atlikti kiti asmenys (paslaugų teikėjų specialistai), diegimas gali būti atliekamas suderinus su Policijos departamento Policijos informacijos valdyba ir prižiūrint administratoriams;

26.2. diegti ir naudoti programinę įrangą, nesusijusią su POLIS valdytojo ar tvarkytojų veikla ar POLIS naudotojo atliekamomis funkcijomis (žaidimų, bylų siuntimo, internetinių pokalbių programų ir kt.), draudžiama.

27. POLIS naudotojai turi vadovautis „švaraus stalo“ politika:

27.1. nors trumpam paliekant KDV privaloma įjungti slaptažodžiu apsaugotą ekrano užsklandą;

27.2. baigus darbą, reikia uždaryti programų langus ir tvarkingai išjungti kompiuterį;

27.3. baigus darbą, nepalikti ant stalo dokumentų ir duomenų laikmenų, sudėti juos į stalčius, spintas ar lentynas;

27.4. dokumentai, kuriuose pateikiama ypač svarbi informacija, iš spausdintuvų turi būti išimami nedelsiant asmens, kuris inicijavo spausdinimą;

27.5. nebereikalingi svarbūs dokumentai turi būti ne išmetami, o sunaikinami dokumentų naikintuvu.

28. POLIS naudotojų prieiga prie kitų valstybės institucijų arba žinybų kompiuterių tinklų ar interneto turi būti apsaugota užkardomis. Interneto turinys turi būti kontroliuojamas, nepraleidžiant nepageidaujamos informacijos. Už kompiuterių tinklo filtravimo įrangos administravimo koordinavimą ir priežiūrą atsakingas administratorius.

29. Leistinos kompiuterių naudojimo ribos:

29.1. stacionarius kompiuterius leidžiama naudoti tik POLIS valdytojo ir tvarkytojų patalpose;

29.2. POLIS naudotojai kompiuterius naudoja išskirtinai tik tarnybinėms funkcijoms atlikti;

29.3. POLIS naudotojai, tarnybinėms funkcijoms atlikti naudojantys nešiojamuosius kompiuterius, išnešdami juos iš POLIS valdytojo ir tvarkytojų patalpų, norėdami POLIS duomenis perduoti kompiuterių tinklais ne savo darbo vietoje, turi naudoti kompiuterio įjungimo slaptažodį, papildomą POLIS naudotojo tapatybės patvirtinimą ir POLIS duomenų šifravimą, rakinimo įtaisus (pvz., Kensingtono užraktas).

30. Užtikrinant saugų elektroninės informacijos teikimą kitoms valstybės institucijoms ir (ar) gavimą iš jų, naudojamas Saugus valstybinis duomenų perdavimo tinklas. Duomenys teikiami ir (ar) gaunami automatiniu būdu tik pagal duomenų teikimo sutartyse nustatytas specifikacijas ir sąlygas.

31. Pagrindiniai atsarginių duomenų kopijų darymo ir atkūrimo reikalavimai:

31.1. POLIS atsarginės duomenų kopijos turi būti daromos periodiškai (visų duomenų kopija – vieną kartą per savaitę). Atsarginių kopijų laikmenos yra sužymimos nurodant kopijos tipą, datą ir kitą sėkmingam atkūrimui reikiamą informaciją;

31.2. periodiškai (ne rečiau kaip kartą per metus) turi būti bandoma atkurti duomenis iš atsarginių duomenų kopijų. Bandymų eiga ir rezultatai įforminami kopijų darymo žurnale;

31.3. atsarginės duomenų kopijos turi būti saugomos:

31.3.1. trečiosios kategorijos informacinių sistemų – užrakintoje nedegioje spintoje;

31.3.2. antrosios kategorijos informacinių sistemų – užrakintoje nedegioje spintoje, kitose patalpose, nei yra įrenginys, kurio elektroninė informacija buvo nukopijuota, arba kitame pastate;

31.4. už atsarginių duomenų kopijų darymą atsakingą asmenį skiria POLIS valdytojo

vadovas.

IV. REIKALAVIMAI PERSONALUI

32. Saugos įgaliotinis privalo išmanyti informacijos saugos užtikrinimo principus, savo darbe vadovautis saugos reikalavimais, Informacinių sistemų elektroninės informacijos techniniais saugos reikalavimais, taip pat Informacinių technologijų saugos atitikties vertinimo metodika, patvirtinta Lietuvos Respublikos vidaus reikalų ministro 2004 m. gegužės 6 d. įsakymu Nr. 1V-156 (Žin., 2004, Nr. 80-2855), kitais Lietuvos Respublikos ir Europos Sąjungos teisės aktais, reglamentuojančiais saugų duomenų tvarkymą, standartais ir kitais dokumentais, turėti atitinkamą kvalifikaciją, sugebėti prižiūrėti, kaip įgyvendinama saugos politika, taip pat turėti darbo su duomenų bazėmis, operacinėmis sistemomis, taikomosiomis programomis patirties.

33. POLIS administratoriai privalo išmanyti pagrindinius saugos politikos principus, darbą su duomenų perdavimo tinklais, užtikrinti jų saugumą, turėti sisteminių programinių priemonių (*Windows, Unix, Oracle*) administravimo ir priežiūros patirties.

34. POLIS naudotojai turi turėti atitinkamą kvalifikaciją (darbo su kompiuteriu įgūdžiai, informacinių technologijų vartotojų kvalifikacijos kursai, pradinis saugaus darbo su duomenimis mokymas, ECDL (Europos kompiuterio vartotojo pažymėjimas) vartotojo sertifikatas ar pan.) ir patirties (darbo su atitinkamomis operacinėmis sistemomis, taikomosiomis programomis ir pan.).

35. POLIS valdytojas kartu su registrų tvarkymo įstaigomis užtikrina tinkamą saugos įgaliotinio, administratorių ir POLIS naudotojų kvalifikacijos tobulinimą.

36. POLIS naudotojams turi būti nuolat rengiami duomenų saugos mokymai, įvairiais būdais primenama apie saugos problemas (pvz., priminimai elektroniniu paštu, teminių seminarų rengimas, atmintinės ir pan.).

V. POLIS NAUDOTOJŲ SUPAŽINDINIMO SU SAUGOS DOKUMENTAIS PRINCIPAI

37. Tvarkyti POLIS duomenis gali tik POLIS naudotojai, pasirašytinai susipažinę su saugos politika ir saugos politiką įgyvendinančiais teisės aktais.

38. Saugos politika ir saugos politiką įgyvendinantys teisės aktai skelbiami POLIS valdytojo tinklalapyje, kaupiami POLIS teisės aktų duomenų bazėje ir POLIS pagalbos ir mokymų medžiagos skiltyje „Duomenų sauga“ (http://pagalba.policija.lt/help.php?type=DS).

39. POLIS naudotojų ir administratorių supažindinimą su saugos politika kitais saugos politiką įgyvendinančiais teisės aktais ir atsakomybę už šių reikalavimų nesilaikymą organizuoja saugos įgaliotinis. Saugos įgaliotinis supažindinimą atlieka šiais būdais ir terminais:

39.1. su informacija apie saugos politikos ar saugos politiką įgyvendinančių teisės aktų priėmimą, keitimą ar panaikinimą – per 10 darbo dienų nuo teisės akto priėmimo, keitimo ar panaikinimo (informacija pateikiama POLIS pagalbos ir mokymų medžiagos skiltyje „Duomenų sauga“);

39.2. Švietimo ar kvalifikacijos tobulinimo duomenų saugos klausimais, supažindinimą su saugaus darbo su duomenimis būdais – žodžiu, elektroniniu paštu ar telefonu, pildydamas ir atnaujindamas POLIS pagalbos ir mokymų medžiagos skilties „Duomenų sauga“ informaciją;

39.3. atmintines rengia ir atnaujina pagal poreikį, bet ne rečiau kaip kartą per metus.

VI. BAIGIAMOSIOS NUOSTATOS

40. POLIS saugos įgaliotinis, administratoriai ir naudotojai privalo rūpintis

informacinės sistemos ir joje tvarkomos informacijos saugumu. Pažeidę saugos politikos ar saugos politiką įgyvendinančių teisės aktų reikalavimus, atsako įstatymų nustatyta tvarka.

_____