LIETUVOS RESPUBLIKOS
VIDAUS REIKALŲ MINISTRAS

ĮSAKYMAS
DĖL INTEGRUOTOS BAUDŽIAMOJO PROCESO INFORMACINĖS SISTEMOS DUOMENŲ SAUGOS NUOSTATŲ PATVIRTINIMO

2015 m. lapkričio 6 d. Nr. 1V-876
Vilnius

Vadovaudamasis Bendrųjų elektroninės informacijos saugos reikalavimų 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 Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašo patvirtinimo“, 7.1 papunkčiu, 11, 19 ir 26 punktais:

1. Tvirtinu Integruotos baudžiamojo proceso informacinės sistemos duomenų saugos nuostatus (pridedama).

2. Pavedu:

2.1. Informatikos ir ryšių departamentui prie Lietuvos Respublikos vidaus reikalų ministerijos per mėnesį nuo Integruotos baudžiamojo proceso informacinės sistemos duomenų saugos nuostatų (toliau – IBPS duomenų saugos nuostatai) patvirtinimo paskirti Integruotos baudžiamojo proceso informacinės sistemos (toliau – IBPS) pagrindinį saugos įgaliotinį ir IBPS pagrindinį (pagrindinius) administratorių (administratorius);

2.2. Nacionalinei teismų administracijai, Lietuvos Respublikos generalinei prokuratūrai, Policijos departamentui prie Lietuvos Respublikos vidaus reikalų ministerijos, Priešgaisrinės apsaugos ir gelbėjimo departamentui prie Lietuvos Respublikos vidaus reikalų ministerijos, Finansinių nusikaltimų tyrimo tarnybai prie Lietuvos Respublikos vidaus reikalų ministerijos, Valstybės sienos apsaugos tarnybai prie Lietuvos Respublikos vidaus reikalų ministerijos, Kalėjimų departamentui prie Lietuvos Respublikos teisingumo ministerijos, Lietuvos Respublikos specialiųjų tyrimų tarnybai, Muitinės kriminalinei tarnybai, Karo policijai per 3 mėnesius nuo IBPS duomenų saugos nuostatų patvirtinimo paskirti IBPS saugos įgaliotinius ir IBPS administratorius;

2.3. IBPS pagrindiniam saugos įgaliotiniui per 3 mėnesius nuo IBPS duomenų saugos nuostatų patvirtinimo parengti ir pateikti IBPS valdytojui tvirtinti saugos politiką įgyvendinančių dokumentų projektus.

Vidaus reikalų ministras Saulius Skvernelis

SUDERINTA
Lietuvos Respublikos generalinės prokuratūros
2015 m. rugsėjo 23 d. raštu Nr. 17.2.-10992

SUDERINTA
Nacionalinės teismų
administracijos 2015 m. rugsėjo 24 d. raštu
Nr. 4R-2355-(1.13 K)

SUDERINTA
Policijos departamento
prie Lietuvos Respublikos vidaus reikalų ministerijos

2015 m. rugpjūčio 20 d. raštu Nr. 5-S-7759

PATVIRTINTA
Lietuvos Respublikos vidaus reikalų ministro
2015 m. lapkričio 6 d. įsakymu Nr. 1V-876

INTEGRUOTOS BAUDŽIAMOJO PROCESO INFORMACINĖS SISTEMOS DUOMENŲ SAUGOS NUOSTATAI

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Integruotos baudžiamojo proceso informacinės sistemos duomenų saugos nuostatai (toliau – Saugos nuostatai) nustato Integruotos baudžiamojo proceso informacinės sistemos (toliau – IBPS) elektroninės informacijos saugos politiką, organizacines, technines, programines, teisines ir kitas priemones, užtikrinančias saugų IBPS elektroninės informacijos tvarkymą.

2. Saugos nuostatuose vartojamos sąvokos apibrėžtos Integruotos baudžiamojo proceso informacinės sistemos nuostatuose, patvirtintuose Lietuvos Respublikos vidaus reikalų ministro, Lietuvos Respublikos generalinio prokuroro ir Nacionalinės teismų administracijos direktoriaus 2012 m. rugsėjo 27 d. įsakymu Nr. 1V-702/I-294/6P-101-(1.1) „Dėl Integruotos baudžiamojo proceso informacinės sistemos įsteigimo ir jos nuostatų patvirtinimo“ (toliau – IBPS nuostatai), 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“ (toliau – Saugos reikalavimų aprašas).

3. IBPS elektroninės informacijos saugos politika įgyvendinama pagal IBPS valdytojo tvirtinamus IBPS saugos politiką įgyvendinančius dokumentus:

3.1. IBPS saugaus elektroninės informacijos tvarkymo taisykles;

3.2. IBPS veiklos tęstinumo valdymo planą;

3.3. IBPS naudotojų administravimo taisykles.

4. IBPS elektroninės informacijos saugos užtikrinimo tikslas – sudaryti sąlygas saugiai automatiniu būdu tvarkyti IBPS elektroninę informaciją, užtikrinti IBPS elektroninės informacijos konfidencialumą, prieinamumą, vientisumą ir tinkamą kompiuterizuotų darbo vietų bei tinklo įrangos funkcionavimą. IBPS elektroninės informacijos saugai užtikrinti kompleksiškai naudojamos administracinės, techninės ir programinės priemonės, padedančios įgyvendinti reagavimo, atsakomybės, suvokimo apie elektroninės informacijos saugos poreikį kėlimo ir saugos priemonių projektavimo ir diegimo principus.

5. IBPS elektroninės informacijos saugos užtikrinimo prioritetinės kryptys:

5.1. IBPS elektroninės informacijos konfidencialumo, vientisumo ir prieinamumo užtikrinimas;

5.2. IBPS elektroninės informacijos tvarkymo kontrolė;

5.3. asmens duomenų apsauga;

5.4. IBPS veiklos tęstinumas.

6. Saugos nuostatai taikomi IBPS valdytojui, IBPS tvarkytojams, IBPS saugos įgaliotiniams, IBPS administratoriams ir IBPS naudotojams.

7. IBPS valdytojas – Lietuvos Respublikos vidaus reikalų ministerija (toliau – VRM), Šventaragio g. 2, Vilnius, kuri atlieka IBPS nuostatuose nustatytas funkcijas, o taip pat:

7.1. rengia ir priima IBPS saugos nuostatus, IBPS saugos politiką įgyvendinančius dokumentus, kitus dokumentus, susijusius su elektroninės informacijos sauga, ir jų pakeitimus;

7.2. prižiūri ir kontroliuoja, kad IBPS būtų tvarkoma vadovaujantis Lietuvos Respublikos įstatymais, IBPS nuostatais, Saugos nuostatais, IBPS saugos politiką įgyvendinančiais dokumentais ir kitais teisės aktais;

7.3. priima sprendimus dėl IBPS techninių ir programinių priemonių, būtinų IBPS elektroninės informacijos saugai užtikrinti, įsigijimo, įdiegimo ir modernizavimo;

7.4. nagrinėja IBPS tvarkytojų pasiūlymus dėl IBPS saugos tobulinimo ir priima dėl jų sprendimus;

7.5. priima sprendimą dėl IBPS informacinių technologijų atitikties saugos reikalavimams vertinimo atlikimo;

7.6. vykdo kitas Saugos nuostatų, IBPS nuostatų, Saugos reikalavimų aprašo ir kitų teisės aktų, reglamentuojančių IBPS elektroninės informacijos tvarkymo teisėtumą ir saugos valdymą, nustatytas funkcijas.

8. IBPS tvarkytojas – Informatikos ir ryšių departamentas prie Lietuvos Respublikos vidaus reikalų ministerijos (toliau – Informatikos ir ryšių departamentas), Šventaragio g. 2, Vilnius, kuris atlieka IBPS nuostatuose nustatytas funkcijas, o taip pat:

8.1. užtikrina tinkamą IBPS saugos dokumentų nuostatų ir IBPS valdytojo rekomendacijų įgyvendinimą;

8.2. užtikrina nepertraukiamą IBPS veikimą ir elektroninės informacijos, esančios IBPS centrinėje duomenų bazėje, saugą;

8.3. skiria IBPS pagrindinį saugos įgaliotinį ir IBPS pagrindinį (pagrindinius) administratorių (administratorius);

8.4. vykdo kitas Saugos nuostatų, Saugos reikalavimų aprašo ir kitų teisės aktų nustatytas funkcijas.

9. Kiti IBPS tvarkytojai, nurodyti IBPS nuostatų 12 punkte, išskyrus teritorines ir specializuotas policijos įstaigas, areštines, kardomojo kalinimo ir pataisos įstaigas, Lietuvos teismus, atlieka IBPS nuostatuose nustatytas funkcijas, o taip pat:

9.1. užtikrina tvarkytojo įstaigos ir tvarkytojo įstaigos reguliavimo ar veiklos sričiai priskirtų kitų įstaigų (teritorinių, specializuotų, atskaitingų ir kitų) IBPS naudotojų darbo vietose naudojamų administracinių, techninių ir programinių priemonių, užtikrinančių elektroninės informacijos saugą, diegimo koordinavimą ir priežiūrą;

9.2. kiekvienas paskiria IBPS saugos įgaliotinį ir IBPS administratorių;

9.3. vykdo kitas Saugos nuostatų, Saugos reikalavimų aprašo ir kitų teisės aktų nustatytas funkcijas.

10. Visi IBPS tvarkytojai užtikrina tvarkytojo įstaigoje tvarkomos IBPS elektroninės informacijos saugą. IBPS tvarkytojų vadovai atsako už reikiamų administracinių, techninių ir organizacinių saugos priemonių įgyvendinimą, užtikrinimą ir laikymąsi Saugos nuostatuose ir IBPS duomenų saugos politiką įgyvendinančiuose dokumentuose nustatyta tvarka.

11. IBPS tvarkytojo – Informatikos ir ryšių departamento – paskirtas IBPS pagrindinis saugos įgaliotinis:

11.1. koordinuoja IBPS tvarkytojų saugos įgaliotinių veiklą, supažindina juos su Saugos nuostatais, IBPS saugos politiką įgyvendinančiais dokumentais, kitais Saugos nuostatų 38 punkte nurodytais dokumentais ir atsakomybe už juose nustatytų reikalavimų nesilaikymą;

11.2. rengia IBPS saugos politiką įgyvendinančių dokumentų projektus;

11.3. koordinuoja ir prižiūri IBPS elektroninės informacijos saugos politikos įgyvendinimą;

11.4. koordinuoja IBPS elektroninės informacijos saugos incidentų tyrimą;

11.5. teikia pasiūlymus Informatikos ir ryšių departamento direktoriui ir IBPS valdytojui dėl:

11.5.1. saugos dokumentų – Saugos nuostatų ir IBPS saugos politiką įgyvendinančių dokumentų – priėmimo, keitimo ar panaikinimo;

11.5.2. IBPS informacinių technologijų atitikties saugos reikalavimams vertinimo atlikimo;

11.5.3. IBPS pagrindinio (pagrindinių) administratoriaus (administratorių) paskyrimo;

11.6. teikia IBPS saugos įgaliotiniams, IBPS pagrindiniam (pagrindiniams) administratoriui (administratoriams) ir IBPS administratoriams, prireikus ir kitiems IBPS valdytojo ir tvarkytojų darbuotojams privalomus vykdyti nurodymus ir pavedimus, susijusius su IBPS saugos politikos įgyvendinimu;

11.7. kasmet organizuoja IBPS saugos įgaliotinių, IBPS administratorių saugos mokymus, reguliariai jiems primena saugos problemas, teikia konsultacijas (elektroniniu paštu, telefonu, prireikus rengia atmintines IBPS naudotojams ir pan.);

11.8. vykdo kitas Saugos nuostatų, IBPS nuostatų, Saugos reikalavimų aprašo ir kitų teisės aktų nustatytas funkcijas.

12. IBPS saugos įgaliotiniai – IBPS tvarkytojų, nurodytų Saugos nuostatų 9 punkte, vadovų paskirti saugos įgaliotiniai:

12.1. koordinuoja ir prižiūri IBPS elektroninės informacijos saugos politikos įgyvendinimą tvarkytojo įstaigoje bei tvarkytojo įstaigos reguliavimo ar veiklos sričiai priskirtose kitose įstaigose (teritorinėse, specializuotose, atskaitingose ir kitose), turinčiose IBPS naudotojų darbo vietas;

12.2. teikia pasiūlymus tvarkytojų vadovams dėl IBPS administratorių paskyrimo;

12.3. teikia IBPS pagrindiniam saugos įgaliotiniui siūlymus dėl:

12.3.1. saugos dokumentų – Saugos nuostatų ir IBPS saugos politiką įgyvendinančių dokumentų – priėmimo, keitimo ar panaikinimo;

12.3.2. IBPS informacinių technologijų atitikties saugos reikalavimams vertinimo atlikimo;

12.3.3. saugos mokymų organizavimo;

12.4. teikia savo tvarkytojo įstaigos ir jos reguliavimo ar veiklos sričiai priskirtų kitų įstaigų IBPS naudotojams privalomus vykdyti nurodymus ir pavedimus, susijusius su IBPS saugos politikos įgyvendinimu;

12.5. informuoja IBPS pagrindinį saugos įgaliotinį apie IBPS elektroninės informacijos saugos incidentus ir teikia siūlymus dėl minėtų incidentų pašalinimo;

12.6. supažindina savo tvarkytojo įstaigos ir jos reguliavimo ar veiklos sričiai priskirtų kitų įstaigų IBPS administratorius ir IBPS naudotojus su Saugos nuostatais, IBPS saugos politiką įgyvendinančiais dokumentais, kitais Saugos nuostatų 38 punkte nurodytais dokumentais ir atsakomybe už juose nustatytų reikalavimų nesilaikymą; supažindinimo su šiame punkte nurodytais dokumentais būdą pasirenka patys IBPS saugos įgaliotiniai, tačiau turi būti užtikrintas susipažinimo įrodomumas;

12.7. kasmet organizuoja savo tvarkytojo įstaigos ir jos reguliavimo ar veiklos sričiai priskirtų kitų įstaigų IBPS administratorių ir IBPS naudotojų saugos mokymus, reguliariai jiems primena saugos problemas, teikia konsultacijas (elektroniniu paštu, telefonu, prireikus rengia atmintines IBPS naudotojams ir pan.). Saugos mokymai organizuojami po to, kai IBPS tvarkytojų vadovų paskirtus saugos įgaliotinius apmoko IBPS pagrindinis saugos įgaliotinis;

12.8. dalyvauja tiriant IBPS tvarkytojo elektroninės informacijos saugos incidentus;

12.9. atlieka kitas Saugos nuostatuose ir kituose saugos politiką įgyvendinančiuose dokumentuose nustatytas funkcijas, susijusias su IBPS elektroninės informacijos sauga.

13. IBPS pagrindinis (pagrindiniai) administratorius (administratoriai):

13.1. prižiūri IBPS ir jos infrastruktūrą, užtikrina jos veikimą ir IBPS elektroninės informacijos saugą;

13.2. pagal kompetenciją registruoja IBPS naudotojus, sukuria ar panaikina naudotojų teises, taip pat suteikia teisę kitiems IBPS administratoriams administruoti savo tvarkytojo įstaigos bei tvarkytojo įstaigos reguliavimo ar veiklos sričiai priskirtų kitų įstaigų (teritorinių, specializuotų, atskaitingų ir kitų) IBPS naudotojus;

13.3. koordinuoja kitų IBPS administratorių veiklą.

14. IBPS administratoriai – tvarkytojų, nurodytų Saugos nuostatų 9 punkte, vadovų paskirti administratoriai:

14.1. atsako už IBPS funkcionavimą užtikrinančios techninės ir programinės įrangos, infrastruktūros ir informacinių technologijų paslaugų administravimą tvarkytojo įstaigoje bei tvarkytojo įstaigos reguliavimo ar veiklos sričiai priskirtose kitose įstaigose (teritorinėse, specializuotose, atskaitingose ir kitose), turinčiose IBPS naudotojų darbo vietas;

14.2. pagal kompetenciją registruoja IBPS elektroninės informacijos saugos incidentus, informuoja apie juos IBPS saugos įgaliotinį ir teikia pasiūlymus dėl šių incidentų pašalinimo;

14.3. pagrindiniam (pagrindiniams) IBPS administratoriui (administratoriams) suteikus teisę, registruoja IBPS naudotojus tvarkytojo įstaigoje bei tvarkytojo įstaigos reguliavimo ar veiklos sričiai priskirtose kitose įstaigose (teritorinėse, specializuotose, atskaitingose ir kitose), turinčiose IBPS naudotojų darbo vietas, ir suteikia IBPS naudotojams prieigos teisę naudotis IBPS infrastruktūra paskirtoms funkcijoms atlikti;

14.4. atlieka kitas Saugos nuostatuose ir saugos politiką įgyvendinančiuose dokumentuose nustatytas funkcijas ir vykdo IBPS saugos įgaliotinio nurodymus, susijusius su IBPS duomenų sauga.

15. IBPS elektroninė informacija tvarkoma ir jos sauga užtikrinama vadovaujantis:

15.1. Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymu;

15.2. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymu;

15.3. Saugos reikalavimų aprašu;

15.4. Techniniais valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimais, patvirtintais Lietuvos Respublikos vidaus reikalų ministro 2013 m. spalio 4 d. įsakymu Nr. 1V-832 „Dėl Techninių valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimų patvirtinimo“;

15.5. Bendraisiais reikalavimais organizacinėms ir techninėms asmens duomenų saugumo priemonėms, patvirtintais Valstybinės duomenų apsaugos inspekcijos direktoriaus 2008 m. lapkričio 12 d. įsakymu Nr. 1T-71(1.12) „Dėl Bendrųjų reikalavimų organizacinėms ir techninėms asmens duomenų saugumo priemonėms patvirtinimo“ (toliau – Bendrieji reikalavimai saugumo priemonėms);

15.6. Lietuvos standartais LST ISO/IEC 27001:2013, LST ISO/IEC 27002:2014, taip pat kitais Lietuvos ir tarptautiniais „Informacijos technologija. Saugumo technika“ grupės standartais, apibūdinančiais informacijos saugos valdymą ir saugų duomenų tvarkymą;

15.7. kitais teisės aktais, reglamentuojančiais elektroninės informacijos tvarkymo teisėtumą ir elektroninės informacijos saugos valdymą.

II SKYRIUS
ELEKTRONINĖS INFORMACIJOS SAUGOS VALDYMAS

16. IBPS tvarkoma elektroninė informacija priskiriama ypatingos svarbos elektroninės informacijos kategorijai vadovaujantis Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo 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 Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašo patvirtinimo“ (toliau – Klasifikavimo gairės), 4.1.2 ir 4.1.7 papunkčiuose nustatytais kriterijais.

17. Atsižvelgiant į IBPS tvarkomos elektroninės informacijos svarbos kategoriją ir vadovaujantis Klasifikavimo gairių 5.1 papunkčiu, IBPS priskiriama pirmajai informacinių sistemų kategorijai.

18. IBPS asmens duomenų tvarkymas automatiniu būdu priskirtinas trečiajam saugumo lygiui vadovaujantis Bendrųjų reikalavimų saugumo priemonėms 11.3 papunkčio nuostata.

19. IBPS pagrindinis saugos įgaliotinis, atsižvelgdamas į VRM išleistą metodinę priemonę „Rizikos analizės vadovas“, Lietuvos ir tarptautinius „Informacijos technologija. Saugumo technika“ grupės standartus, kasmet organizuoja IBPS rizikos įvertinimą ir parengia rizikos įvertinimo ataskaitą; prireikus jis gali organizuoti neeilinį rizikos įvertinimą.

20. IBPS rizikos įvertinimo ataskaita rengiama atsižvelgiant į rizikos veiksnius, galinčius turėti įtakos informacijos saugai. Svarbiausi rizikos veiksniai:

20.1. subjektyvūs netyčiniai (duomenų tvarkymo klaidos ir apsirikimai, duomenų ištrynimas, klaidingas duomenų teikimas, duomenų perdavimo tinklų veiklos trikdymai, programinės įrangos klaidos, netinkamas veikimas ir kita);

20.2. subjektyvūs tyčiniai (nesankcionuotas naudojimasis informacinėmis sistemomis, duomenų pakeitimas ir sunaikinimas, duomenų perdavimo tinklų veiklos trikdymai, fizinio saugumo pažeidimai, vagystės ir kita);

20.3. veiksniai, nurodyti Atleidimo nuo atsakomybės esant nenugalimos jėgos (force majeure) aplinkybėms taisyklių, patvirtintų Lietuvos Respublikos Vyriausybės 1996 m. liepos 15 d. nutarimu Nr. 84 „Dėl Atleidimo nuo atsakomybės esant nenugalimos jėgos (*force majeure*) aplinkybėms taisyklių patvirtinimo“, 3 punkte.

21. IBPS valdytojas, atsižvelgdamas į IBPS rizikos įvertinimo ataskaitą, prireikus tvirtina Informatikos ir ryšių departamento parengtą rizikos įvertinimo ir rizikos valdymo priemonių planą, kuriame numatomas techninių, administracinių ir kitų išteklių poreikis rizikos valdymo priemonėms įgyvendinti.

22. Siekdamas užtikrinti Saugos nuostatuose ir IBPS saugos politiką įgyvendinančiuose dokumentuose nustatytų reikalavimų įgyvendinimo organizavimą ir kontrolę, IBPS pagrindinis saugos įgaliotinis ne rečiau kaip kartą per metus organizuoja IBPS informacinių technologijų saugos atitikties vertinimą, kurio metu:

22.1. įvertinama realios IBPS elektroninės informacijos saugos situacijos atitiktis Saugos nuostatų, IBPS saugos politiką įgyvendinančių dokumentų ir kitų teisės aktų reikalavimams;

22.2. patikrinama ne mažiau kaip 10 procentų atsitiktinai parinktų IBPS naudotojų kompiuterizuotų darbo vietų bei visų tarnybinių stočių įdiegta programinė įranga ir jos sąranka;

22.3. patikrinama (įvertinama) IBPS naudotojams ir administratoriams suteiktų teisių atitiktis vykdomoms funkcijoms;

22.4. įvertinamas pasirengimas užtikrinti IBPS veiklos tęstinumą įvykus elektroninės informacijos saugos incidentui.

23. Ne rečiau kaip kartą per trejus metus IBPS informacinių technologijų saugos atitikties vertinimą turi atlikti nepriklausomi, visuotinai pripažintų tarptautinių organizacijų sertifikuoti informacinių sistemų auditoriai.

24. Atlikus IBPS informacinių technologijų saugos atitikties vertinimą, IBPS saugos įgaliotinis rengia pastebėtų trūkumų šalinimo planą, kurį tvirtina, atsakingus vykdytojus paskiria ir nustatytų trūkumų šalinimo įgyvendinimo terminus nustato IBPS valdytojo vadovas.

25. Pagrindiniai elektroninės informacijos saugos priemonių parinkimo principai yra šie:

25.1. likutinė rizika turi būti sumažinta iki priimtino lygio;

25.2. elektroninės informacijos saugos priemonės diegimo kaina turi būti proporcinga saugomos elektroninės informacijos vertei;

25.3. turi būti įdiegtos prevencinės, detekcinės ir korekcinės informacijos saugos priemonės.

III SKYRIUS
ORGANIZACINIAI IR TECHNINIAI REIKALAVIMAI

26. Programinės įrangos, skirtos IBPS apsaugoti nuo kenksmingos programinės įrangos (virusų, programinės įrangos, skirtos šnipinėjimui, nepageidaujamo elektroninio pašto ir panašiai), naudojimo nuostatos ir jos atnaujinimo reikalavimai:

26.1. IBPS tarnybinėse stotyse ir kompiuterizuotose darbo vietose turi būti naudojamos centralizuotai valdomos kenksmingos programinės įrangos aptikimo priemonės, nuolat ieškančios ir blokuojančios kenksmingą programinę įrangą (virusų, šnipinėjimo programinę įrangą ir kt.), kurios turi būti reguliariai atnaujinamos automatiniu būdu ne rečiau kaip kartą per 24 valandas;

26.2. programinės įrangos konfigūravimas turi būti apsaugotas slaptažodžiu.

27. Programinės įrangos, įdiegtos tarnybinėse stotyse ir kompiuterizuotose darbo vietose, naudojimo nuostatos:

27.1. IBPS darbui gali būti naudojama tik legali ir patikrinta programinė įranga;

27.2. programinė įranga atnaujinama laikantis gamintojo reikalavimų;

27.3. programinės įrangos diegimą, šalinimą ir konfigūravimą atlieka IBPS pagrindinis (pagrindiniai) administratorius (administratoriai) arba kitų IBPS tvarkytojų paskirti IBPS administratoriai (atsižvelgiant į programinės įrangos diegimo, šalinimo ar konfigūravimo vietą).

28. Kompiuterių tinklo filtravimo įrangos (užkardų, turinio kontrolės sistemų, įgaliotųjų serverių (angl. *proxy*) ir kt.) pagrindinės naudojimo nuostatos:

28.1. kompiuterių tinklai nuo viešųjų telekomunikacijų tinklų (interneto) turi būti atskirti ugniasienėmis, DOS ir DDOS atakų prevencijai skirta įranga bei įsilaužimų aptikimo ir prevencijos įranga;

28.2. visas duomenų srautas į internetą ir iš jo yra filtruojamas naudojant apsaugą nuo virusų ir kitos kenksmingos programinės įrangos;

28.3. naudojamos turinio filtravimo sistemos.

29. Metodai, kuriais leidžiama užtikrinti saugų elektroninės informacijos teikimą ir (ar) gavimą:

29.1. IBPS naudotojų, jų vykdytų užklausų ir peržiūrėtų užklausų rezultatų duomenys tvarkomi Vidaus reikalų informacinės sistemos naudotojų administravimo posistemėje Lietuvos Respublikos vidaus reikalų ministro 2005 m. kovo 9 d. įsakymu Nr. 1V-68 „Dėl Vidaus reikalų informacinės sistemos centrinio duomenų banko duomenų peržiūros kontrolės taisyklių patvirtinimo“ nustatyta tvarka;

29.2. prieiga prie IBPS elektroninės informacijos suteikiama įgyvendinus IBPS naudotojų administravimo taisyklėse nustatytas IBPS naudotojų autentifikavimo priemones. Tiesioginė prieiga prie IBPS užtikrinama automatiniu būdu ištisą parą darbo ir poilsio dienomis;

29.3. IBPS elektroninė informacija perduodama automatiniu būdu naudojant TCP/IP protokolą realiame laike *(On-line* režimu) arba asinchroniniu režimu pagal IBPS duomenų teikimo sutartis, kuriose nustatytos perduodamos elektroninės informacijos specifikacijos, kopijų skaičius, kitos elektroninės informacijos perdavimo sąlygos ir tvarka;

29.4. IBPS elektroninė informacija, perduodama ne per IBPS tvarkytojams priklausančias duomenų perdavimo linijas, privalo būti šifruojama.

30. IBPS elektroninės informacijos perdavimui naudojamas Vidaus reikalų telekomunikacinis tinklas ir Saugus valstybinis duomenų perdavimo tinklas.

31. IBPS naudotojams, savo tarnybinėms funkcijoms vykdyti naudojantiems nešiojamus kompiuterius IBPS elektroninės informacijos perdavimui kompiuterių tinklais ne savo darbo vietoje, šiuose kompiuteriuose turi būti naudojamas kompiuterio įjungimo slaptažodis, papildomas IBPS naudotojo tapatybės patvirtinimas ir elektroninės informacijos šifravimas.

32. IBPS naudotojams, kuriems būtinas prisijungimas tiesioginėms pareigoms atlikti iš nutolusios darbo vietos, gali būti suteikiama nuotolinio prisijungimo prie IBPS galimybė:

32.1. 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);

32.2. prie IBPS prisijungiama nuotoliniu būdu naudojant interneto naršyklę (https protokolą).

33. Pagrindiniai atsarginių elektroninės informacijos kopijų darymo ir atkūrimo reikalavimai:

33.1. IBPS elektroninės informacijos kopijos turi būti daromos automatiškai kiekvieną dieną. Prireikus jas atkurti turi teisę IBPS pagrindinis (pagrindiniai) administratorius (administratoriai);

33.2. atkūrimas iš elektroninės informacijos kopijų privalo būti išbandomas;

33.3. elektroninės informacijos kopijos turi būti saugomos kitoje patalpoje nei IBPS tarnybinės stotys.

IV SKYRIUS
REIKALAVIMAI PERSONALUI

34. IBPS pagrindinis saugos įgaliotinis ir IBPS saugos įgaliotiniai privalo išmanyti elektroninės informacijos saugos užtikrinimo principus, privalo tobulinti kvalifikaciją elektroninės informacijos saugos srityje.

35. IBPS administratoriai privalo išmanyti pagrindinius elektroninės informacijos saugos principus, turėti sisteminių programinių priemonių administravimo ir priežiūros patirties, mokėti administruoti ir prižiūrėti duomenų bazes.

36. IBPS naudotojai privalo turėti darbo su kompiuteriu įgūdžių, mokėti tvarkyti IBPS elektroninę informaciją IBPS nuostatų nustatyta tvarka, būti susipažinę su Saugos nuostatais bei IBPS saugos politiką įgyvendinančiais dokumentais ir sutikę laikytis jų reikalavimų. IBPS naudotojai turi būti mokomi dirbti su specialia programine įranga, reikalinga jų darbo funkcijoms atlikti.

37. IBPS naudotojams turi būti nuolat rengiami duomenų saugos mokymai, įvairiais būdais primenama apie saugos problematiką (pvz., priminimai elektroniniu paštu, teminių seminarų rengimas, atmintinės ir pan.). Saugos mokymai organizuojami kasmet, mokymus organizuoja IBPS pagrindinis saugos įgaliotinis ir IBPS saugos įgaliotiniai, apmokyti IBPS pagrindinio saugos įgaliotinio ir suderinę su juo mokymų temas. Po mokymų įvertinamas jų efektyvumas.

V SKYRIUS
IBPS NAUDOTOJŲ SUPAŽINDINIMO SU SAUGOS DOKUMENTAIS PRINCIPAI

38. Tvarkyti IBPS elektroninę informaciją gali tik IBPS naudotojai, susipažinę su Saugos nuostatais, IBPS saugos politiką įgyvendinančiais dokumentais ir kitais teisės aktais, kuriais vadovaujamasi tvarkant elektroninę informaciją, užtikrinant jos saugumą, atsakomybe už saugos dokumentų nuostatų pažeidimus, ir raštu sutikę laikytis saugos dokumentuose nustatytų reikalavimų. Pakartotinis supažindinimas yra vykdomas pasikeitus minėtiems dokumentams ir teisės aktams.

39. Už IBPS naudotojų supažindinimą pagal kompetenciją yra atsakingi IBPS pagrindinis saugos įgaliotinis ir IBPS saugos įgaliotiniai.

40. Saugos nuostatai ir IBPS saugos politiką įgyvendinantys dokumentai iš esmės turi būti persvarstomi (peržiūrimi) ne rečiau kaip kartą per kalendorinius metus. IBPS saugos dokumentai turi būti persvarstomi (peržiūrimi) atlikus rizikos veiksnių analizę ar informacinių technologijų saugos atitikties vertinimą arba įvykus esminiams organizaciniams, sisteminiams ar kitiems pokyčiams. Saugos įgaliotinis atsakingas, kad IBPS naudotojai būtų informuoti apie IBPS saugos dokumentų pakeitimą ir (ar) pripažinimą netekusiais galios.

VI SKYRIUS
BAIGIAMOSIOS NUOSTATOS

41. IBPS tvarkytojai, IBPS saugos įgaliotiniai, IBPS administratoriai ir IBPS naudotojai, pažeidę Saugos nuostatų ar kitų saugų elektroninės informacijos tvarkymą reglamentuojančių teisės aktų reikalavimus, atsako Lietuvos Respublikos įstatymų ir kitų teisės aktų nustatyta tvarka.

_____