



LIETUVOS RESPUBLIKOS VIDAUS REIKALŲ MINISTRAS

ĮSAKYMAS

**DĖL INTEGRUOTOS BAUDŽIAMOJO PROCESO INFORMACINĖS SISTEMOS
SAUGAUS ELEKTRONINĖS INFORMACIJOS TVARKYMO TAISYKLIŲ,
INTEGRUOTOS BAUDŽIAMOJO PROCESO INFORMACINĖS SISTEMOS VEIKLOS
TĘSTINUMO VALDYMO PLANO IR INTEGRUOTOS BAUDŽIAMOJO PROCESO
INFORMACINĖS SISTEMOS NAUDOTOJŲ ADMINISTRAVIMO TAISYKLIŲ
PATVIRTINIMO**

2016 m. vasario 1 d. Nr. 1V-73

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“, 8 punktu,

t v i r t i n u pridedamas:

1. Integruotos baudžiamojo proceso informacinės sistemos saugaus elektroninės informacijos tvarkymo taisyklės;
2. Integruotos baudžiamojo proceso informacinės sistemos veiklos tęstinumo valdymo planą;
3. Integruotos baudžiamojo proceso informacinės sistemos naudotojų administravimo taisyklės.

Vidaus reikalų ministras

Saulius Skvernelis

**INTEGRUOTOS BAUDŽIAMOJO PROCESO INFORMACINĖS SISTEMOS SAUGOS
ELEKTRONINĖS INFORMACIJOS TVARKYMO
TAISYKLĖS**

**I SKYRIUS
BENDROSIOS NUOSTATOS**

1. Integruotos baudžiamojo proceso informacinės sistemos saugos elektroninės informacijos tvarkymo taisyklės (toliau – Taisyklės) nustato tvarką, užtikrinančią saugų Integruotos baudžiamojo proceso informacinės sistemos (toliau – IBPS) elektroninės informacijos tvarkymą.

2. Taisyklėse vartojamos sąvokos atitinka sąvokas, vartojamas 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, registų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašo patvirtinimo“, 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), Integruotos baudžiamojo proceso informacinės sistemos duomenų saugos nuostatuose, patvirtintuose Lietuvos Respublikos vidaus reikalų ministro 2015 m. lapkričio 6 d. įsakymu Nr. 1V-876 „Dėl Integruotos baudžiamojo proceso informacinės sistemos duomenų saugos nuostatų patvirtinimo“ (toliau – Saugos nuostatai).

3. IBPS tvarkoma elektroninė informacija ir jos grupės nurodytos IBPS nuostatų III skyriuje.

4. Už IBPS elektroninės informacijos tvarkymą atsakingi:

4.1. IBPS naudotojai – už elektroninės informacijos, kurią tvarkyti jiems suteiktos teisės, tvarkymą;

4.2. IBPS administratoriai – už IBPS naudojamų klasifikatorių ir IBPS naudotojų duomenų tvarkymą.

**II SKYRIUS
TECHNINIŲ IR KITŲ SAUGOS PRIEMONIŲ APRAŠYMAS**

5. Kompiuterinės įrangos saugos priemonės:

5.1. tarnybinės stotys apsaugomos nuo elektros srovės nutrūkimo ir svyravimų;

5.2. patalpose, kuriose yra techninė įranga, užtikrinamos gamintojo nustatytos techninės įrangos darbo sąlygos;

5.3. visa techninė įranga į tarnybinių stočių patalpas įnešama ir išnešama iš jų tik už techninės įrangos priežiūrą atsakingam asmeniui leidus;

5.4. tiesioginė prieiga prie tarnybinių stočių suteikiama tik pagrindiniams IBPS administratoriams, išskyrus atvejus, kai, atliekant techninės ir programinės įrangos paleidimo, derinimo ar kitus darbus, Informatikos ir ryšių departamento prie Lietuvos Respublikos vidaus reikalų ministerijos specialiųjų patalpų įėjimo ir išėjimo kontrolės organizavimo taisyklių, patvirtintų Informatikos ir ryšių departamento prie Lietuvos Respublikos vidaus reikalų ministerijos direktoriaus 2010 m. gruodžio 7 d. įsakymu Nr. 5V-33 „Dėl Informatikos ir ryšių departamento prie Lietuvos Respublikos vidaus reikalų ministerijos specialiųjų patalpų įėjimo ir išėjimo kontrolės organizavimo taisyklių patvirtinimo“ (toliau – Specialiųjų patalpų įėjimo ir išėjimo kontrolės organizavimo taisyklės), nustatyta tvarka ji gali būti suteikta asmeniui, atliekančiam nurodytus darbus;

5.5. svarbiausia kompiuterinė įranga, duomenų perdavimo tinklo mazgai ir ryšio linijos turi būti dubliuoti ir jų techninė būklė nuolat stebima;

5.6. svarbiausios kompiuterinės įrangos gedimai turi būti registruojami, taip pat turi būti paskirtas už gedimų registravimą atsakingas asmuo;

5.7. kitos kompiuterinės įrangos saugos priemonės yra nustatytos Saugos nuostatuose, kituose teisės aktuose, reglamentuojančiuose saugų valstybės informacinių išteklių elektroninės informacijos tvarkymą.

6. Sisteminės ir taikomosios programinės įrangos saugos priemonės:

6.1. slaptažodžiai, leidžiantys dirbti su IBPS tarnybinių stočių programine įranga, yra žinomi tik IBPS administratoriams ir saugomi seife, užklijuotame voke;

6.2. IBPS naudojama tik legali, patikimų gamintojų programinė įranga;

6.3. programinės įrangos diegimą, konfigūravimą ir šalinimą atlieka tik pagrindinis IBPS administratorius ir Informatikos ir ryšių departamento prie Lietuvos Respublikos vidaus reikalų ministerijos (toliau – Informatikos ir ryšių departamentas) valstybės tarnautojas, pagal pareigybės aprašymą atsakingas už taikomąją programinę įrangą;

6.4. programinė įranga prižiūrima laikantis gamintojo rekomendacijų;

6.5. programinės įrangos testavimas atliekamas naudojant atskirą testavimo aplinką;

6.6. naudojamos vykdomo kodo kontrolės priemonės, automatiškai apribojančios ar informuojančios apie neautorizuoto programinio kodo vykdymą;

6.7. naudojamos priemonės, automatiškai informuojančios IBPS administratorius apie pradelstą kenkėjiškos programinės įrangos aptikimo priemonių atnaujinimo laiką;

6.8. pagrindinių tarnybinių stočių įvykių žurnaluose (angl. *event log*), apsaugotuose nuo neteisėto juose esančių duomenų naudojimo, keitimo, iškraipymo, sunaikinimo, registruojami ir ne trumpiau nei 1 metus saugomi duomenys apie: IBPS įjungimą, išjungimą, sėkmingus ir nesėkmingus bandymus registruotis ir prieiti prie informacinių išteklių, visus IBPS naudotojų vykdomus veiksmus, kitus svarbius saugai įvykius, nurodant IBPS naudotojo identifikatorių ir įvykio laiką. Šie duomenys analizuojami ne rečiau nei kartą per savaitę ar įvykus saugos incidentui. Už šių duomenų registravimą, saugojimą, analizavimą yra atsakingi ir jie yra prieinami tik pagrindiniams IBPS administratoriams ir pagrindiniam IBPS saugos įgaliotiniui.

6.9. IBPS naudotojui neatliekant jokių veiksmų IBPS ilgiau nei 15 minučių, IBPS taikomoji programinė įranga užsirakina; toliau naudotis IBPS galima tik pakartotinai patvirtinus savo tapatybę;

6.10. kitos saugos priemonės, susijusios su IBPS programinės įrangos sauga, nustatytos Saugos nuostatuose, kituose saugų elektroninės informacijos tvarkymą reglamentuojančiuose teisės aktuose.

7. IBPS elektroninės informacijos perdavimo tinklais saugumo užtikrinimo priemonės:

7.1. nuotolinis prisijungimas prie informacinės sistemos turi būti vykdomas protokolu, skirtu duomenų šifravimui;

7.2. informacinės sistemos elektroninės informacijos perdavimo tinklas turi būti atskirtas nuo viešųjų ryšių tinklų naudojant ugniasienę; ugniasienės įvykių žurnalai (angl. *Logs*) turi būti reguliariai analizuojami, o ugniasienės saugumo taisyklės periodiškai peržiūrimos ir atnaujinamos;

7.3. kitos duomenų perdavimo tinklais saugumo užtikrinimo priemonės yra nustatytos Saugos nuostatuose, kituose saugų elektroninės informacijos tvarkymą reglamentuojančiuose teisės aktuose.

8. Patalpų ir aplinkos saugumo užtikrinimas:

8.1. Patekimo į IBPS tarnybinių stočių patalpas ir patalpas, kuriose saugomos atsarginės elektroninės informacijos kopijos, sąlygos nustatytos Specialiųjų patalpų įėjimo ir išėjimo kontrolės organizavimo taisyklėse;

8.2. pasirenkant tarnybinių stočių vietą pastate, atsižvelgiama į transporto keliamą vibraciją, galimą eismo įvykių poveikį, arti esančius radijo siųstuvus ir kt.;

8.3. prieigai prie patalpų, kuriose yra tarnybinės stotys, kontroliuoti naudojama vaizdo stebėjimo sistema;

8.4. visos išorinės durys ir langai tarnybinių stočių patalpose tinkamai apsaugomi nuo neleistinos prieigos;

8.5. patalpos, kuriose yra tarnybinės stotys, atskiriamos nuo bendrojo naudojimo patalpų; į šias patalpas patekti gali tik Specialiųjų patalpų įėjimo ir išėjimo kontrolės organizavimo taisyklių 4 punkte nurodyti įgalioti asmenys, kitus asmenis lydi įgaliotieji asmenys;

8.6. durys į patalpas, kuriose yra tarnybinės stotys, yra šarvuotos;

8.7. tarnybinių stočių patalpose įrengiamas šildymas, vėdinimas ir oro kondicionavimas; šiose patalpose įrengiamos gaisro signalizacijos ir automatinės gaisro gesinimo sistemos, palaikomas tarnybinių stočių gamintojų nustatytas santykinis oro drėgnumas;

8.8. patalpose, kuriose yra tarnybinės stotys, įdiegiama signalizacija, nustatoma įeinančių ir išėinančių iš patalpų asmenų tapatybė (pvz., elektroninės tapatybės nustatymo kortelės ir pan.);

8.9. ryšių kabeliai apsaugomi nuo neteisėto prisijungimo ar pažeidimo.

9. Kitos priemonės, naudojamos užtikrinti IBPS elektroninės informacijos saugą:

9.1. įdiegiama IBPS tarnybinių stočių, IBPS centrinės duomenų bazės stebėjimo sistema, siekiant užtikrinti nepertraukiamą IBPS funkcionavimą, automatinį techninės ir programinės įrangos sutrikimų nustatymą ir informavimą apie tai;

9.2. naudojantis programine įranga, nuolat atliekama IBPS funkcionavimo analizė ir IBPS funkcionavimo sutrikimų prevencija;

9.3. saugos reikalavimų atitikties vertinimas atliekamas ne rečiau kaip vieną kartą per metus, o ne rečiau kaip kartą per trejus metus atitikties vertinimą turi atlikti nepriklausomi, visuotinai pripažintų tarptautinių organizacijų sertifikuoti informacinių sistemų auditoriai;

9.4. turi būti įgyvendinti Lietuvos standarte LST ISO/IEC 27002:2014 nurodytas saugos priemonės, išskyrus priemones, kurios netaikytinos dėl institucijos veiklos, informacinės sistemos ar naudojamos informacinėje sistemoje techninės įrangos pobūdžio, ir Lietuvos standarte LST ISO/IEC 27001:2013 nurodytus reikalavimus informacijos saugumo valdymo sistemai;

9.5. per metus IBPS prieinamumas turi būti užtikrintas ne mažiau kaip 99 proc. laiko visą parą;

9.6. IBPS neveikimo laikotarpis negali būti ilgesnis nei 8 valandos.

III SKYRIUS SAUGUS ELEKTRONINĖS INFORMACIJOS TVARKYMAS

10. Saugaus IBPS elektroninės informacijos įvedimo, keitimo, atnaujinimo ir naikinimo tvarka:

10.1. IBPS tvarkomus duomenis įvesti, keisti, atnaujinti ar atlikti kitus tvarkymo veiksmus gali tik IBPS naudotojas pagal suteiktas prieigos teises;

10.2. IBPS naudotojų duomenis įvesti, keisti, atnaujinti gali tik pagrindinis IBPS administratorius ir (arba) IBPS tvarkytojų administratoriai, kuriems suteikta IBPS naudotojų administravimo teisė pagal Saugos nuostatų 14.3 papunktį;

10.3. klasifikatorių duomenų bazėje tvarkomus duomenis įvesti, keisti, atnaujinti gali tik IBPS administratorius pagal suteiktas prieigos teises;

10.4. duomenys IBPS gali būti tvarkomi tik turint teisėtą pagrindą;

10.5. duomenų įvedimas, pakeitimas, atnaujinimas registruojami šių Taisyklių 6.8 papunktyje nustatyta tvarka;

10.6. duomenys naikinami IBPS nuostatų 45 punkte nustatyta tvarka.

11. Atsarginės IBPS elektroninės informacijos kopijos daromos Saugos nuostatų 33 punkte nustatyta tvarka.

12. IBPS elektroninės informacijos atkūrimo iš atsarginių IBPS elektroninės informacijos kopijų bandymus testinėje versijoje ne rečiau kaip kartą per ketvirtį atlieka pagrindinis IBPS administratorius.

13. IBPS elektroninė informacija kitiems registrams ir informacinėms sistemoms teikiama ir gaunama iš jų tik pasirašius duomenų teikimo sutartis, laikantis šių reikalavimų:

13.1. IBPS elektroninė informacija kitiems registrams ir informacinėms sistemoms perduodama vadovaujantis IBPS nuostatais ir kitais saugų elektroninės informacijos tvarkymą reglamentuojančiais teisės aktais;

13.2. duomenų teikėjai į IBPS elektroninę informaciją turi teikti Lietuvos Respublikos vidaus reikalų ministro ir Lietuvos Respublikos generalinio prokuroro tvirtinamo Baudžiamosios bylos duomenų tvarkymo elektronine forma ikiteisminio tyrimo metu tvarkos aprašo nustatytais būdais, apimtimi, reguliarumu ir terminais.

14. Neteisėto duomenų kopijavimo, keitimo, naikinimo ar perdavimo nustatymo tvarka:

14.1. IBPS naudotojai, pastebėję saugos dokumentų reikalavimų pažeidimus, nusikalstamos veikos požymius, neveikiančias arba netinkamai veikiančias duomenų saugos užtikrinimo priemones, privalo nedelsdami pranešti apie tai IBPS naudotojų administravimo taisyklių 10 punkte nustatyta tvarka ir imtis visų įmanomų prevencinių veiksmų, siekiant užkirsti kelią neteisėtam duomenų naudojimui.

15. IBPS programinės ir techninės įrangos keitimo ir atnaujinimo tvarka:

15.1. IBPS tarnybinėse stotyse programinę įrangą, reikalingą IBPS darbui, diegia ir tvarko pagrindiniai IBPS administratoriai;

15.2. IBPS darbui reikalinga taikomoji programinė įranga perkama su visomis autorinėmis teisėmis (programos išeities kodais ir teisėmis juos keisti), nustatomas garantinio aptarnavimo laikas trūkumams ir klaidoms pašalinti;

15.3. organizuojami IBPS naudotojų darbo su nauja programine ir technine įranga mokymai;

15.4. naudojama tik sertifikuota programinė ir techninė įranga;

15.5. sugedusią techninę įrangą išvežant remontuoti, išimamos duomenų laikmenos (kietieji diskai ir kt.) arba daromos jų kopijos ir laikmenose saugomi duomenys ištrinami;

15.6. techninės, programinės ir sisteminės įrangos naujinimui galioja pokyčių valdymo tvarka;

15.7. IBPS programinės ir techninės įrangos keitimo ir atnaujinimo tvarką su trečia šalimi, jei šiai šaliai Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymo 41 straipsnyje nustatytais sąlygomis ir tvarka perduotos informacinės sistemos ir (ar) jos infrastruktūros priežiūros funkcijos (toliau – paslaugų teikėjas), priklausomai nuo konkretaus atvejo, derina pagrindinis IBPS administratorius arba ji aprašoma paslaugų, susijusių su IBPS programinės ir techninės įrangos keitimu ir atnaujinimu, teikimo sutartyse.

16. IBPS pokyčių valdymo tvarka:

16.1. IBPS valdytojas užtikrina IBPS pokyčių (toliau – pokyčiai) valdymo planavimą, apimančią pokyčių identifikavimą, suskirstymą į kategorijas pagal pokyčio tipą (administracinis, organizacinis ar techninis), įtakos vertinimą (svarbumas ir skubumas), pokyčių prioritetų nustatymo (eiliškumas) procesus;

16.2. pokyčiai identifikuojami nustatčius IBPS naudotojų, IBPS administratorių poreikius, apibendrinus kylančias priežiūros problemas ir kitais gerosios praktikos įvardinamais atvejais;

16.3. visi potencialūs pokyčiai registruojami pokyčių registre, įvertinus ir valdytojui patvirtinus įtakos vertinimą ir prioritetą;

16.4. visi pokyčiai (projektavimas, kūrimas, testavimas, diegimas) atliekami tik IBPS valdytojo iniciatyva, IBPS saugos įgaliotinio ar IBPS administratoriaus iniciatyva;

16.5. pokyčių projektavimą ir kūrimą atlieka Informatikos ir ryšių departamento valstybės tarnautojas, pagal pareigybės aprašymą atsakingas už taikomosios programinės įrangos priežiūrą ir projektavimą tam skirtoje kūrimo aplinkoje, reikalui esant pasitelkdamas trečiąsias šalis;

16.6. prieš atliekant pokyčius, kurių metu gali iškilti grėsmė elektroninės informacijos konfidencialumui, vientisumui ar pasiekiamumui, visi pokyčiai turi būti išbandomi testavimo aplinkoje, kuri yra identiška gamybinei aplinkai;

16.7. įgyvendinant pokyčius, kurių metu galimi IBPS veikimo sutrikimai, pagrindinis IBPS administratorius privalo ne vėliau kaip prieš dvi darbo dienas iki planuojamų pokyčių pradžios (elektroniniu paštu, faksu ar kitomis priemonėmis) informuoti IBPS tvarkytojų administratorius ir savo administruojamus IBPS naudotojus apie tokių darbų pradžią ir galimus

sutrikimus; IBPS tvarkytojų administratoriai nedelsdami apie tai informuoja savo administruojamus IBPS naudotojus.

16.8. atlikęs pokyčių testavimą, jei ir testavimo darbų dėl programinių ir (ar) techninių priežasčių nebuvo galima atlikti, IBPS administratorius gali pradėti eksploatuoti pakeitimus;

16.9. jeigu testavimas sėkmingas, pokyčiai perkeliama į gamybinę aplinką;

16.10. visi pokyčiai registruojami ir apie tai informuojami IBPS administratoriai ir IBPS naudotojai;

16.11. Pagrindinis IBPS administratorius savo administruojamiems IBPS naudotojams ir IBPS tvarkytojų administratoriams privalo pateikti visą reikalingą informaciją apie naudojimosi IBPS pakitimus. IBPS tvarkytojų administratoriai apie šiuos pokyčius informuoja savo administruojamus IBPS naudotojus.

17. IBPS naudotojams savo tarnybinėms funkcijoms vykdyti skirtų nešiojamų kompiuterių ir kitų mobiliųjų įrenginių (toliau – mobilieji įrenginiai) naudojimo tvarką nustato IBPS tvarkytojo vadovas. Šios tvarkos apraše turi būti nustatyta:

17.1. mobiliųjų įrenginių apskaitos tvarkymas;

17.2. mobiliųjų įrenginių skyrimo ir naudojimo tvarka;

17.3. operacinės sistemos ir taikomosios programinės įrangos saugos atnaujinimo reikalavimai;

17.4. kenksmingos programinės įrangos aptikimo priemonės;

17.5. techninio aptarnavimo sąlygos.

IV SKYRIUS

REIKALAVIMAI, KELIAMU IBPS FUNKCIONUOTI REIKALINGOMS PASLAUGOMS IR JŲ TEIKĖJAMS

18. Pagrindinis IBPS administratorius atsako už programinių, techninių ir kitų prieigos prie IBPS resursų organizavimą, suteikimą ir panaikinimą techninės ir (ar) programinės paslaugos teikėjui.

19. IBPS administratorius suteikia paslaugos teikėjui tik tokią prieigą prie IBPS resursų, kuri yra būtina norint atlikti arba vykdyti sutartyje nustatytus įsipareigojimus, kurie neprieštarauja įstatymų ir kitų teisės aktų reikalavimams.

20. IBPS administratorius privalo supažindinti paslaugos teikėjus su suteiktos prieigos prie informacinės sistemos reikalavimais ir sąlygomis.

21. Pasibaigus sutarties su paslaugos teikėjais galiojimo terminui ar atsiradus kitoms sutartyje ar IBPS saugos politiką įgyvendinančiuose dokumentuose įvardintoms sąlygoms, IBPS administratorius nedelsdamas privalo panaikinti suteiktą prieigą.

22. Reikalavimai, keliami patalpoms, įrangai, informacinės sistemos priežiūrai, duomenų perdavimui tinklais ir kitoms paslaugoms, turi atitikti šiose Taisyklėse nustatytus reikalavimus.

V SKYRIUS BAIGIAMOSIOS NUOSTATOS

23. IBPS naudotojai, IBPS administratoriai, IBPS saugos įgaliotiniai, pažeidę šių Taisyklių reikalavimus, atsako teisės aktų nustatyta tvarka.

INTEGRUOTOS BAUDŽIAMOJO PROCESO INFORMACINĖS SISTEMOS VEIKLOS TĘSTINUMO VALDYMO PLANAS

I SKYRIUS BENDROSIOS NUOSTATOS

1. Integruotos baudžiamojo proceso informacinės sistemos veiklos tęstinumo valdymo planas (toliau – Planas) reglamentuoja Integruotos baudžiamojo proceso informacinės sistemos (toliau – IBPS) administratorių, IBPS saugos įgaliotinių, IBPS naudotojų veiksmus įvykus elektroninės informacijos saugos incidentui (toliau – incidentas).

2. Plane vartojamos sąvokos atitinka sąvokas, vartojamas 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 – Bendrųjų saugos reikalavimų aprašas), 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), Integruotos baudžiamojo proceso informacinės sistemos duomenų saugos nuostatuose, patvirtintuose Lietuvos Respublikos vidaus reikalų ministro 2015 m. lapkričio 6 d. įsakymu Nr. 1V-876 „Dėl Integruotos baudžiamojo proceso informacinės sistemos duomenų saugos nuostatų patvirtinimo“ (toliau – Saugos nuostatai).

3. Planas įsigalioja įvykus incidentui ir yra privalomas IBPS valdytojui, IBPS tvarkytojams, IBPS saugos įgaliotiniams, IBPS administratoriams bei IBPS naudotojams.

4. IBPS administratoriai, IBPS saugos įgaliotiniai, IBPS naudotojai incidento metu turi visus įgaliojimus atlikti veiksmus, nurodytus IBPS veiklos atkūrimo detalajame plane (Plano 1 priedas) (toliau – detalusis planas). IBPS administratoriai, IBPS saugos įgaliotiniai, prireikus – IBPS naudotojai nedelsdami šalina elektroninės informacijos saugos incidento padarinius ir įgyvendina kitas detalajame plane numatytus veiksmus.

5. IBPS veiklos atkūrimas, įvykus incidentui, finansuojamas iš Lietuvos Respublikos valstybės biudžeto ir kitų finansavimo šaltinių. Finansinių ir kitokių išteklių, numatomų IBPS

veiklai atkurti, paskelbus incidentą, šaltinius ir pobūdį numato ir pasirenka IBPS veiklos tęstinumo valdymo grupė (toliau – Valdymo grupė).

6. IBPS veiklos kriterijai, pagal kuriuos galima nustatyti, ar IBPS veikla atkurta, yra šie:

6.1. IBPS naudotojai gali atlikti savo darbines funkcijas IBPS įprastiniu būdu;

6.2. užtikrintas elektroninės informacijos IBPS prieinamumas, konfidencialumas ir vientisumas;

6.3. IBPS vykdo IBPS nuostatuose ir kituose teisės aktuose nurodytus uždavinius ir funkcijas.

II SKYRIUS ORGANIZACINĖS NUOSTATOS

7. Valdymo grupė užtikrina veiklos tęstinumui kylančių grėsmių valdymą ir IBPS atkūrimo koordinavimą įvykus incidentui.

8. Valdymo grupę sudaro:

8.1. Informatikos ir ryšių departamento prie Lietuvos Respublikos vidaus reikalų ministerijos (toliau – Informatikos ir ryšių departamentas) direktoriaus pavaduotojas (Valdymo grupės vadovas);

8.2. Informatikos ir ryšių departamento Sistemų administravimo ir naudotojų pagalbos skyriaus vedėjas (Valdymo grupės vadovo pavaduotojas);

8.3. Informatikos ir ryšių departamento Saugos skyriaus vedėjas;

8.4. Informatikos ir ryšių departamento Telekomunikacinio tinklo administravimo skyriaus vedėjas;

8.5. Informatikos ir ryšių departamento Projektų ir sistemų strateginio valdymo skyriaus vedėjas;

8.6. Informatikos ir ryšių departamento paskirtas pagrindinis IBPS saugos įgaliotinis (toliau – pagrindinis IBPS saugos įgaliotinis);

8.7. IBPS tvarkytojų paskirti saugos įgaliotiniai;

8.8. IBPS tvarkytojo vadovo sprendimu paskirtas atstovas (-ai), kai incidentas kilo dėl IBPS tvarkytojo (-ų) IBPS naudotojų veiklos;

8.9. kiti Informatikos ir ryšių departamento direktoriaus įsakymu paskirti specialistai arba pagal sutartį veikiantys juridinių asmenų atstovai.

9. Valdymo grupės funkcijos:

9.1. situacijos analizė ir sprendimų IBPS veiklos tęstinumo valdymo klausimais priėmimas;

- 9.2. bendravimas su viešosios informacijos rengėjų ir viešosios informacijos skleidėjų atstovais;
- 9.3. bendravimas su susijusių registrų / informacinių sistemų veiklos tęstinumo valdymo grupėmis;
- 9.4. bendravimas su teisėsaugos ir kitomis institucijomis, institucijos darbuotojais ir kitomis interesų grupėmis;
- 9.5. finansinių ir kitų išteklių, reikalingų IBPS veiklai atkurti, įvykus incidentui, naudojimo kontrolė;
- 9.6. elektroninės informacijos fizinė sauga įvykus incidentui;
- 9.7. logistika (žmonių, daiktų, įrangos gabenimas ir jo organizavimas);
- 9.8. IBPS veiklos atkūrimo priežiūra ir koordinavimas;
- 9.9. kitos Valdymo grupei pavestos funkcijos.
10. IBPS veiklos atkūrimo grupė (toliau – Atkūrimo grupė) vykdo IBPS atkūrimo darbus ir Valdymo grupės nurodymus, susijusius su IBPS funkcionalumo atkūrimu.
11. Atkūrimo grupę sudaro:
 - 11.1. Informatikos ir ryšių departamento direktoriaus pavaduotojas (Atkūrimo grupės vadovas);
 - 11.2. Informatikos ir ryšių departamento Sistemų administravimo ir naudotojų pagalbos skyriaus Naudotojų pagalbos poskyrio vedėjas (Atkūrimo grupės vadovo pavaduotojas);
 - 11.3. Informatikos ir ryšių departamento Informacijos apdorojimo ir statistikos skyriaus vedėjas;
 - 11.4. Informatikos ir ryšių departamento Projektų ir sistemų strateginio valdymo skyriaus Informacinių technologijų taikymo poskyrio vedėjas;
 - 11.5. Informatikos ir ryšių departamento Telekomunikacinio tinklo administravimo skyriaus Telefono ryšio ir duomenų perdavimo tinklų poskyrio vedėjas;
 - 11.6. Informatikos ir ryšių departamento Sistemų administravimo ir naudotojų pagalbos skyriaus Sistemų administravimo poskyrio vyriausiasis specialistas (specialistai);
 - 11.7. Informatikos ir ryšių departamento Sistemų administravimo ir naudotojų pagalbos skyriaus Naudotojų pagalbos poskyrio vyresnysis specialistas;
 - 11.8. Informatikos ir ryšių departamento Telekomunikacinio tinklo administravimo skyriaus Telefono ryšio ir duomenų perdavimo tinklų poskyrio vyriausiasis specialistas;
 - 11.9. Informatikos ir ryšių departamento paskirtas pagrindinis IBPS administratorius (toliau – pagrindinis IBPS administratorius);
 - 11.10. IBPS tvarkytojų paskirti IBPS administratoriai;

11.11. kiti Informatikos ir ryšių departamento direktoriaus įsakymu paskirti specialistai arba pagal sutartį veikiantys juridinių asmenų atstovai;

11.12. išoriniai ekspertai (jei būtina).

12. Atkūrimo grupės funkcijos:

12.1. tarnybinių stočių veikimo atkūrimo organizavimas;

12.2. kompiuterių tinklo veikimo atkūrimo organizavimas;

12.3. IBPS elektroninės informacijos atkūrimo organizavimas;

12.4. taikomųjų programų tinkamo veikimo atkūrimo organizavimas;

12.5. darbo kompiuterių veikimo atkūrimo ir prijungimo prie kompiuterių tinklo organizavimas;

12.6. kitos Atkūrimo grupei pavestos funkcijos.

13. Valdymo grupė ir Atkūrimo grupė tarpusavyje ir su kitomis grupėmis bendrauja naudodamosi elektroninių ryšių priemonėmis: elektroniniu paštu, mobiliuoju ryšiu ir kitomis įmanomomis ryšio priemonėmis. Bendravimo dažnumą, įvertinusi incidento mastą, pobūdį ir veiklos atkūrimo eigą, nustato Valdymo grupė pirmojo susitikimo metu. Bendraujama tol, kol bus pašalinti incidento padariniai.

14. Reaguojant į incidentus ir juos valdant, turi būti vadovaujamasi veiksmais, išdėstytais detalajame plane.

15. Incidento metu sunaikinta techninė, sisteminė ir taikomoji programinė įranga keičiama turima rezervine arba testine IBPS aplinkos įranga, vėliau įsigyjama Lietuvos Respublikos viešųjų pirkimų įstatymo nustatyta tvarka, įsigijimo išteklių padengiami iš Lietuvos Respublikos valstybės biudžeto ir kitų finansavimo šaltinių.

16. Atsarginių patalpų, naudojamų veiklai atkurti, įvykus incidentui, reikalavimai:

16.1. patekimas į patalpas registruojamas žurnale;

16.2. patalpos atskirtos nuo bendrojo naudojimo patalpų;

16.3. patalpos atitinka priešgaisrinės saugos reikalavimus, jose įrengtos gaisro gesinimo priemonės;

16.4. patalpų durys šarvuotos ir apsaugotos skirtingos konstrukcijos spynomis;

16.5. patalpose įrengtas rezervinis elektros energijos šaltinis, užtikrinantis įrangos veikimą ne trumpiau kaip 30 minučių;

16.6. patalpoje nuolat veikia oro temperatūros ir drėgmės reguliavimo įranga (oro kondicionavimo sistema);

16.7. Jeigu pagrindinės patalpos, kuriose yra IBPS tarnybinės stotys ir kita telekomunikacinė įranga, yra netinkamos, siekiant užtikrinti IBPS veiklą įvykus incidentui, naudojamos atsarginės IBPS atkūrimo patalpos, esančios Žirmūnų g. 1D, Vilniuje.

III SKYRIUS

APRAŠOMOSIOS NUOSTATOS

17. IBPS informacinių technologijų įrangos sąrašai ir jos parametrai nurodyti IBPS techniniame aprašyme (specifikacijoje) ir detalaus projektavimo dokumente. Pagal pareigybių aprašymus už šios įrangos priežiūrą atsakingas IBPS administratorius.

18. IBPS administratorių pavaduojančio asmens minimalus kompetencijos ar žinių lygis negali būti žemesnis už IBPS administratoriui keliamų reikalavimų, nustatytų jo pareigybės aprašyme, lygi.

19. Patalpų brėžinius ir šiose patalpose esančios įrangos bei komunikacijų sąrašą (jame pažymint tarnybines stotis, kompiuterių tinklo ir telefonų tinklo mazgus, kompiuterių tinklo ir telefonų tinklo laidų vedimo tarp pastato aukštų vietas, elektros įvedimo pastate vietas) parengia ir saugo IBPS administratoriai.

20. Duomenų teikimo bei kompiuterinės, techninės ir programinės įrangos priežiūros sutartis pagal kompetenciją saugo atsakingi Informatikos ir ryšių departamento Informacijos apdorojimo ir statistikos skyriaus bei Valdymo organizavimo ir personalo skyriaus vyriausieji specialistai.

21. Programinės įrangos laikmenos ir laikmenos su atsarginėmis duomenų kopijomis saugomos užrakintoje nedegioje spintoje, kitose patalpose, nei yra įrenginys, kurio elektroninė informacija buvo nukopijuota. Atsarginės duomenų kopijos yra perkeliamos į saugojimo vietą kartą per savaitę.

22. Pagrindinis IBPS saugos įgaliotinis ir pagrindinis IBPS administratorius (pagrindiniai IBPS administratoriai) parengia ir saugo sąrašus su Valdymo grupės ir Atkūrimo grupės narių tarnybinių mobiliųjų telefonų numeriais.

IV SKYRIUS

PLANO VEIKSMINGUMO IŠBANDYMO NUOSTATOS

23. Pagrindinis IBPS saugos įgaliotinis Plano veiksmingumo paskutinio ir kito planuojamo išbandymo būdą ir datą nurodo Plano veiksmingumo išbandymų registracijos žurnale, kurio forma nustatyta Plano 2 priede.

24. Planas turi būti išbandomas ne rečiau kaip kartą per metus. Plano veiksmingumas išbandomas incidento teorinio modeliavimo, simuliacinio žaidimo ar kitu būdu.

25. Pagal bandymų rezultatus pagrindinis IBPS saugos įgaliotinis parengia IBPS veiklos tęstinumo valdymo plano veiksmingumo išbandymo ataskaitą (toliau – Ataskaita) (Plano 3 priedas), kurioje yra apibendrinami atliktų bandymų rezultatai, akcentuojami pastebėti trūkumai ir pasiūlomos šių trūkumų šalinimo priemonės. Pagrindinis IBPS saugos įgaliotinis ataskaitą pateikia IBPS valdytojui.

26. Plano veiksmingumo išbandymo metu pastebėti trūkumai šalinami remiantis operatyvumo, veiksmingumo ir ekonomiškumo principais.

Integruotos baudžiamojo proceso informacinės sistemos
veiklos tęstinumo valdymo plano
1 priedas

**INTEGRUOTOS BAUDŽIAMOJO PROCESO INFORMACINĖS SISTEMOS VEIKLOS ATKŪRIMO
DETALUSIS PLANAS**

Elektroninės informacijos saugos incidentas	Veiksmai esant elektroninės informacijos saugos incidentui	IBPS veiklos atkūrimo veiksmai	IBPS veiklos atkūrimo veiksmų atsakingi vykdytojai
1. Gamtinės sąlygos (klimatinių sąlygų pakitimai)	1.1. galimos žalos IBPS įvertinimas, priemonių plano užkirsti kelią elektroninės informacijos saugos incidentui (toliau – saugos incidentas) sudarymas ir įgyvendinimas;	1.1.1. žalos įvertinimas, priemonių plano saugos incidento pasekmėms likviduoti sudarymas ir įgyvendinimas;	Veiklos tęstinumo valdymo grupės vadovas
	1.2. IBPS veiklos atkūrimo veiksmus atliekančių darbuotojų paskyrimas, jų budėjimo grafiko nustatymas ir jų informavimas apie tai;	1.2.1. darbų grafiko saugos incidento pasekmėms likviduoti sudarymas; 1.2.2. saugos incidento pasekmių likvidavimo darbams atlikti darbuotojų sąrašo sudarymas ir jų informavimas apie tai;	IBPS administratorius Veiklos atkūrimo grupės vadovas IBPS administratorius
	1.3. meteorologinės informacijos sekimas;	1.3.1. saugos incidento pasekmių likvidavimo darbus atliekančių darbuotojų informavimas apie esamą situaciją;	IBPS saugos įgaliotinis
	1.4. IBPS naudotojams rekomenduojamo elgesio saugos incidento metu skelbimas žodžiu arba ryšio priemonėmis;	1.4.1. saugos incidento pasekmių likvidavimo darbus atliekančių darbuotojų instruktavimas apie elgseną saugos incidento vietoje;	IBPS saugos įgaliotinis

Elektroninės informacijos saugos incidentas	Veiksmai esant elektroninės informacijos saugos incidentui	IBPS veiklos atkūrimo veiksmai	IBPS veiklos atkūrimo veiksmų atsakingi vykdytojai
	1.5. saugios vietos nustatymas ir nurodymas IBPS naudotojams eiti į saugią vietą;	1.5.1. IBPS naudotojų informavimas apie būtinumą pereiti į kitas saugias patalpas;	Veiklos tęstinumo valdymo grupės vadovas
	1.6. IBPS naudotojų informavimas apie darbo sustabdymą dėl nepalankių sąlygų;	1.6.1. IBPS naudotojų informavimas apie esamą situaciją ir numatomas darbo sąlygas;	IBPS saugos įgaliotinis
	1.7. pasiruošimas suteikti nukentėjusiems IBPS naudotojams pirmąją pagalbą;	1.7.1. pirmos pagalbos suteikimas nukentėjusiems IBPS naudotojams, nukentėjusių gabenimo į gydymo įstaigą organizavimas;	IBPS administratorius
	1.8. pavojingų vietų ženklavimas, informacinių lentelių pakabinimas;	1.8.1. IBPS naudotojų informavimas, saugos incidento pasekmes likviduojančių darbuotojų instruktavimas;	IBPS saugos įgaliotinis
	1.9. alternatyvių energijos tiekimo šaltinių panaudojimas;	1.9.1. energijos tiekimo tarnybų rekomendacijų vykdymas;	Veiklos atkūrimo grupės vadovas
	1.10. alternatyvaus ryšio organizavimas;	1.10.1. kreipimasis į ryšio paslaugos teikėjus;	Veiklos atkūrimo grupės vadovas
	1.11. pagrindinės IBPS techninės ir programinės įrangos, duomenų galimam pavojui išvengti / likviduoti paruošimas;	1.11.1. IBPS tarnybinių stočių, kitos techninės įrangos išjungimas;	IBPS administratorius
2. Potvynis	2.1. veiksmų, nurodytų šio priedo 1.1, 1.2, 1.4 papunkčiuose, atlikimas;	2.1.1. veiksmų, nurodytų šio priedo 1.1.1, 1.2.1, 1.2.2 1.3.1, 1.4.1 papunkčiuose, atlikimas;	Veiklos tęstinumo valdymo grupės vadovas IBPS saugos įgaliotinis

Elektroninės informacijos saugos incidentas	Veiksmai esant elektroninės informacijos saugos incidentui	IBPS veiklos atkūrimo veiksmai	IBPS veiklos atkūrimo veiksmų atsakingi vykdytojai
			IBPS administratorius
	2.2. potvynio prognozės sekimas;	2.2.1. Saugos incidento pasekmės likviduojančių darbuotojų instruktavimas;	IBPS saugos įgaliotinis
	2.3. veiksmų, nurodytų šio priedo 1.5–1.11 papunkčiuose, atlikimas;	2.3.1. IBPS naudotojų informavimas apie būtinumą pereiti į kitas saugias patalpas;	Veiklos tęstinumo valdymo grupės vadovas
		2.3.2. IBPS naudotojų informavimas apie esamą situaciją ir numatomas darbo sąlygas;	IBPS saugos įgaliotinis
		2.3.3. pirmos pagalbos suteikimas nukentėjusiems IBPS naudotojams, nukentėjusių gabenimo į gydymo įstaigą organizavimas;	IBPS administratorius
		2.3.4. IBPS naudotojų informavimas, saugos incidento pasekmės likviduojančių darbuotojų instruktavimas;	IBPS saugos įgaliotinis
		2.3.5. energijos tiekimo tarnybų rekomendacijų vykdymas;	Veiklos atkūrimo grupės vadovas
		2.3.6. kreipimasis į ryšio paslaugos teikėjus;	Veiklos atkūrimo grupės vadovas
		2.3.7. IBPS tarnybinių stočių, kitos techninės įrangos išjungimas;	IBPS administratorius
	2.4. IBPS naudotojų, dirbančių potvynio vietoje,	2.4.1. IBPS naudotojų, dirbančių potvynio	IBPS saugos įgaliotinis

Elektroninės informacijos saugos incidentas	Veiksmai esant elektroninės informacijos saugos incidentui	IBPS veiklos atkūrimo veiksmai	IBPS veiklos atkūrimo veiksmų atsakingi vykdytojai
	aprūpinimas karštu maistu;	vietoje, maitinimo organizavimas;	
3. Pavojingos medžiagos	3.1. pavojingų medžiagų šalinimo tarnybos informavimas;	3.1.1. pavojingų medžiagų šalinimo tarnybos paklausimas dėl leidimo dirbti saugos incidento zonoje, rekomendacijų darbui gavimas ir IBPS naudotojų informavimas apie rekomenduojamus darbo būdus;	Veiklos testinumo valdymo grupės vadovas
	3.2. priešgaisrinės apsaugos ir gelbėjimo tarnybos informavimas;	3.2.1. priešgaisrinės apsaugos ir gelbėjimo tarnybos paklausimas dėl leidimo dirbti saugos incidento vietoje;	IBPS saugos įgaliotinis
	3.3. esant būtinumui IBPS naudotojų evakuacija;	3.3.1. galimybių evakuoti IBPS naudotojus nagrinėjimas, jei gauta priešgaisrinės apsaugos ir gelbėjimo tarnybos rekomendacija;	Veiklos testinumo valdymo grupės vadovas IBPS saugos įgaliotinis
	3.4. veiksmų, nurodytų šio priedo 1.1, 1.2, 1.4–1.11 papunkčiuose, atlikimas;	3.4.1. veiksmų, nurodytų šio priedo 1.1.1, 1.2.1, 1.2.2, 1.4.1–1.11.1 papunkčiuose, atlikimas;	Veiklos testinumo valdymo grupės vadovas IBPS saugos įgaliotinis IBPS administratorius
4. Gaisras	4.1. esant būtinumui, IBPS naudotojų evakuacija;	4.2.1. galimybių evakuoti IBPS naudotojus nagrinėjimas,	Veiklos testinumo valdymo grupės vadovas IBPS saugos įgaliotinis
	4.2. priešgaisrinės apsaugos ir gelbėjimo tarnybos informavimas;	4.2.1. priešgaisrinės ir gelbėjimo tarnybos paklausimas dėl leidimo dirbti saugos incidento zonoje, rekomendacijų darbui gavimas, IBPS naudotojų informavimas	IBPS saugos įgaliotinis

Elektroninės informacijos saugos incidentas	Veiksmai esant elektroninės informacijos saugos incidentui	IBPS veiklos atkūrimo veiksmai	IBPS veiklos atkūrimo veiksmų atsakingi vykdytojai
		apie rekomenduojamus darbo būdus;	
	4.3. gaisro gesinimas ankstyvoje stadijoje, nekeliant pavojaus IBPS naudotojų gyvybei;	4.3.1. priešgaisrinės ir gelbėjimo tarnybos nurodymų vykdymas;	IBPS administratorius
	4.4. komunalinių komunikacijų, galinčių sukelti papildomą nenumatytą situaciją, išjungimas;	4.4.1. priešgaisrinės ir gelbėjimo tarnybos rekomendacijų vykdymas;	IBPS administratorius
	4.5. veiksmų, nurodytų šio priedo 1.1, 1.2, 1.4–1.11 papunkčiuose, atlikimas;	4.5.1. veiksmų, nurodytų šio priedo 1.1.1, 1.2.1, 1.2.2, 1.4.1–1.11.1 papunkčiuose, atlikimas;	Veiklos tęstinumo valdymo grupės vadovas IBPS saugos įgaliotinis IBPS administratorius
5. Patalpų, kuriose yra IBPS tarnybinės stotys ir svarbiausia komutacinė įranga (toliau – patalpos) užgrobimas	5.1. teisėsaugos tarnybų informavimas;	5.1.1. teisėsaugos tarnybų informavimas apie saugos incidentą;	Veiklos tęstinumo valdymo grupės vadovas
	5.2. esant būtinumui, visų konkrečioje situacijoje nereikalingų IBPS naudotojų evakavimas, įspėjant teisėsaugos tarnybas;	5.2.1. IBPS naudotojų informavimas apie evakavimą, jei yra teisėsaugos tarnybų rekomendacija;	IBPS saugos įgaliotinis
	5.3. esant būtinumui, IBPS techninės įrangos išjungimas ir patalpų užrakinimas;	5.3.1. IBPS tarnybinių stočių, kitos techninės įrangos išjungimas, patalpų užrakinimas, jei yra galimybė;	IBPS administratorius
	5.4. esant būtinumui, likusių IBPS naudotojų evakavimas;	5.4.1. IBPS naudotojų informavimas apie evakavimą, jei yra teisėsaugos tarnybų	IBPS saugos įgaliotinis

Elektroninės informacijos saugos incidentas	Veiksmai esant elektroninės informacijos saugos incidentui	IBPS veiklos atkūrimo veiksmai	IBPS veiklos atkūrimo veiksmų atsakingi vykdytojai
		rekomendacija;	
	5.5. teisėsaugos pareigūnų nurodymų vykdymas;	5.5.1. IBPS naudotojų informavimas apie teisėsaugos tarnybų nurodymus;	IBPS saugos įgaliotinis
	5.6. veiksmų, nurodytų šio priedo 1.1, 1.2, 1.4–1.11 papunkčiuose, atlikimas;	5.6.1. veiksmų, nurodytų šio priedo 1.1.1, 1.2.1, 1.2.2, 1.4.1–1.11.1 papunkčiuose, atlikimas;	Veiklos testinimo valdymo grupės vadovas IBPS saugos įgaliotinis IBPS administratorius
6. Patalpų sugadinimas	6.1. avarinių ar teisėsaugos tarnybų informavimas, atsižvelgiant į iškilusio pavojaus pobūdį;	6.1.1. atitinkamos tarnybos paklausimas dėl leidimo dirbti pavojaus zonoje, rekomendacijų darbui gavimas, IBPS naudotojų informavimas apie rekomenduojamus darbo būdus;	IBPS saugos įgaliotinis
	6.2. veiksmų, nurodytų šio priedo 1.1, 1.2, 1.4–1.11 papunkčiuose, atlikimas;	6.2.1. veiksmų, nurodytų šios priedo 1.1.1, 1.2.1, 1.2.2, 1.4.1–1.11.1 papunkčiuose, atlikimas;	Veiklos testinimo valdymo grupės vadovas IBPS saugos įgaliotinis IBPS administratorius
	6.3. esant reikalui, atsarginių patalpų IBPS veiklai užtikrinti ir darbo vietoms išdėstyti suradimas;	6.3.1. darbo organizavimas ir koordinavimas atsarginėse IBPS patalpose;	Veiklos atkūrimo grupės vadovas
	6.4. komunalinių komunikacijų, galinčių sukelti papildomą saugos incidentą, išjungimas;	6.4.1. pažeistų patalpų rekonstrukcijos, atstatymo darbų, komunalinių komunikacijų išjungimo organizavimas ir / ar IBPS perkėlimas į naujas patalpas;	Veiklos testinimo valdymo grupės vadovas Veiklos atkūrimo grupės vadovas
7. Elektros energijos tiekimo sutrikimai	7.1. elektros energijos tiekimo sistemos veiklos patikrinimas;	7.1.1. pažeisto vietos elektros tinklo, užtikrinančio IBPS veiklą, atkūrimo organizavimas;	Veiklos atkūrimo grupės vadovas

Elektroninės informacijos saugos incidentas	Veiksmai esant elektroninės informacijos saugos incidentui	IBPS veiklos atkūrimo veiksmai	IBPS veiklos atkūrimo veiksmų atsakingi vykdytojai
	7.2. esant būtinumui, tarnybinių stočių ir kitos techninės įrangos, jautrios elektros energijos tiekimo sutrikimams, išjungimas;	7.2.1. elektros energijos tiekimo IBPS tarnybinėms stotims ir kitai techninei įrangai išjungimas;	Veiklos atkūrimo grupės vadovas IBPS administratorius
	7.3. kreipimasis į savo elektros energijos tiekimo tarnybą dėl sutrikimo pašalinimo trukmės prognozės;	7.3.1. rekomendacijų iš elektros energijos tiekimo tarnybos gavimas;	Veiklos atkūrimo grupės vadovas
	7.4. sutrikimo pašalinimo trukmės prognozės skelbimas IBPS naudotojams;	7.4.1. IBPS naudotojų informavimas apie esamą situaciją bei numatomas darbo sąlygas;	IBPS saugos įgaliotinis
	7.5. veiksmų, nurodytų šio priedo 1.1, 1.2, 1.4, 1.10, 6.3 papunkčiuose, atlikimas;	7.5.1. veiksmų, nurodytų šio priedo 1.1.1, 1.2.1, 1.2.2, 1.4.1, 1.10.1, 6.3.1 papunkčiuose, vykdymas;	Veiklos testavimo valdymo grupės vadovas IBPS saugos įgaliotinis IBPS administratorius
8. Vandentiekio ir šildymo sistemos sutrikimai	8.1. vandentiekio ar šilumos tinklų avarinių tarnybų informavimas, atsižvelgus į sutrikimo pobūdį;	8.1.1. atitinkamos tarnybos informavimas apie sutrikimus, rekomendacijų darbui gavimas, IBPS naudotojų informavimas apie rekomenduojamus darbo būdus;	Veiklos atkūrimo grupės vadovas IBPS saugos įgaliotinis
	8.2. sutrikimo pašalinimo prognozės skelbimas IBPS naudotojams;	8.2.1. IBPS naudotojų informavimas apie esamą situaciją bei numatomas darbo sąlygas;	IBPS saugos įgaliotinis
	8.3. veiksmų, nurodytų šio priedo 1.1, 1.2, 4.4, 6.3 papunkčiuose, atlikimas;	8.3.1. veiksmų, nurodytų šio priedo 1.1.1, 1.2.1, 4.4.1, 6.3.1 papunkčiuose, atlikimas;	Veiklos testavimo valdymo grupės vadovas IBPS saugos įgaliotinis IBPS administratorius

Elektroninės informacijos saugos incidentas	Veiksmai esant elektroninės informacijos saugos incidentui	IBPS veiklos atkūrimo veiksmai	IBPS veiklos atkūrimo veiksmų atsakingi vykdytojai
9. Ryšio sutrikimai	9.1. ryšio sutrikimo priežasčių nustatymas;	9.1.1. veiksmų, nurodytų šio priedo 1.1.1, 1.2.1, 1.2.2 papunkčiuose, atlikimas;	Veiklos tęstinumo valdymo grupės vadovas Veiklos atkūrimo grupės vadovas IBPS administratorius
	9.2. telefono ir / ar interneto ryšio paslaugų teikėjų informavimas, atsižvelgus į sutrikimo pobūdį, paklausimo dėl jo pašalinimo trukmės prognozės pateikimas;	9.2.1. kreipimasis į telefono ir / ar interneto paslaugų teikėjus;	Veiklos atkūrimo grupės vadovas
	9.3. sutrikimo pašalinimo prognozės skelbimas IBPS naudotojams;	9.3.1. IBPS naudotojų informavimas apie esamą situaciją ir numatomas darbo sąlygas;	IBPS saugos įgaliotinis
	9.4. alternatyvaus ryšio organizavimas;	9.4.1. neatkūrus ryšio per prognozuotą laiką, ryšio per kitus ryšio paslaugų teikėjus organizavimas;	Veiklos atkūrimo grupės vadovas IBPS administratorius
10. IBPS tarnybinių stočių ar komutacinės įrangos sugadinimas (gedimas), sunaikinimas, praradimas	10.1. veiksmų, nurodytų šio priedo 1.1, 1.2, 1.4, 1.6 papunkčiuose, atlikimas;	10.1.1. veiksmų, nurodytų šio priedo 1.1.1, 1.2.1, 1.2.2, 1.4.1, 1.6.1 papunkčiuose, atlikimas;	Veiklos tęstinumo valdymo grupės vadovas IBPS saugos įgaliotinis IBPS administratorius
	10.2. rezervinės IBPS techninės įrangos naudojimas;	10.2.1. esant būtinumui, kreipimasis į teisėsaugos tarnybas dėl IBPS techninės įrangos sugadinimo ar praradimo ir jų nurodymų vykdymas;	Veiklos atkūrimo grupės vadovas

Elektroninės informacijos saugos incidentas	Veiksmai esant elektroninės informacijos saugos incidentui	IBPS veiklos atkūrimo veiksmai	IBPS veiklos atkūrimo veiksmų atsakingi vykdytojai
		10.2.2. pranešimas draudimo įstaigai apie įvykį, dėl kurio nukentėjo apdrausti daiktai;	Veiklos testinumo grupės vadovas
		10.2.3. esamos techninės įrangos išteklių perskirstymas IBPS veiklai užtikrinti;	Veiklos atkūrimo grupės vadovas
		10.2.4. esant būtinumui, kreipimasis į techninės įrangos tiekėjus dėl sugadintos įrangos remonto ar dėl naujos techninės įrangos įsigijimo;	Veiklos atkūrimo grupės vadovas
11. IBPS programinės įrangos sugadinimas, praradimas	11.1. veiksmų, nurodytų šio priedo 1.1, 1.2, 1.4 papunkčiuose, atlikimas;	11.1.1. veiksmų, nurodytų šio priedo 1.1.1, 1.2.1, 1.2.2, 1.4.1 papunkčiuose, atlikimas;	Veiklos testinumo valdymo grupės vadovas IBPS saugos įgaliotinis IBPS administratorius
	11.2. IBPS programinės įrangos atkūrimas iš atsarginių kopijų;	11.2.1. esant būtinumui, kreipimasis į teisėsaugos tarnybas dėl programinės įrangos sugadinimo ar praradimo ir jų nurodymų vykdymas;	Veiklos testinumo valdymo grupės vadovas
		11.2.2. sugadintos ar prarastos programinės įrangos atkūrimas iš programinės įrangos kopijų;	IBPS administratorius
12. IBPS duomenų pakeitimas, sunaikinimas, atskleidimas	12.1. veiksmų, nurodytų šio priedo 1.1, 1.2, 1.4, 1.6 papunkčiuose, atlikimas.	12.1.1. veiksmų, nurodytų šio priedo 1.1.1, 1.2.1, 1.2.2, 1.4.1, 1.6.1 papunkčiuose, atlikimas;	Veiklos testinumo valdymo grupės vadovas IBPS saugos įgaliotinis IBPS administratorius
		12.1.2. įvykus neteisėtam IBPS duomenų	Veiklos testinumo valdymo

Elektroninės informacijos saugos incidentas	Veiksmai esant elektroninės informacijos saugos incidentui	IBPS veiklos atkūrimo veiksmai	IBPS veiklos atkūrimo veiksmų atsakingi vykdytojai
		pakeitimui, sunaikinimui ar atskleidimui, kreipimasis į teisėsaugos tarnybas ir jų nurodymų vykdymas;	grupės vadovas
		12.1.3. IBPS nustojus funkcionuoti dėl duomenų pakeitimo ar sunaikinimo, duomenų atkūrimas iš duomenų kopijų;	IBPS administratorius
		12.1.4. nesant galimybių atkurti pakeistų ar sunaikintų duomenų iš duomenų kopijų, IBPS duomenų gavėjų informavimas dėl būtinumo sugadintus ar prarastus duomenis iš naujo įrašyti į duomenų bazines.	IBPS saugos įgaliotinis

Integruotos baudžiamojo proceso informacinės sistemos
veiklos tęstinumo valdymo plano
2 priedas

(Žurnalo forma)

PLANO VEIKSMINGUMO IŠBANDYMŲ REGISTRACIJOS ŽURNALAS

Eil. Nr.	Plano išbandymo būdas	Data	Atsakingo asmens vardas, pavardė	Atsakingo asmens pareigos
	2	3	4	5

**(Integruotos baudžiamojo proceso informacinės sistemos veiklos testinimo valdymo plano
išbandymo ataskaitos forma)**

**INTEGRUOTOS BAUDŽIAMOJO PROCESO INFORMACINĖS SISTEMOS VEIKLOS
TĖSTINUMO VALDymo PLANO VEIKSMINGUMO IŠBANDYMO ATASKAITA**

(Veiklos testinimo valdymo grupės susitikimo data ir dokumento numeris)

Incidento bandyme dalyvavo Veiklos testinimo valdymo grupės nariai:

1. _____
2. _____
3. _____
- ... _____

Incidento apibūdinimas:

Informacinės sistemos, kurias paveikė Incidentas:

Incidento valdymo eiga:

Rasti Plano trūkumai:

Pasiūlymai keisti arba papildyti Planą:

(vardas, pavardė)

(parašas)

(vardas, pavardė)

(parašas)

(vardas, pavardė)

(parašas)

PATVIRTINTA
Lietuvos Respublikos vidaus reikalų
ministro 2016 m. vasario 1 d.
įsakymu Nr. 1V-73

INTEGRUOTOS BAUDŽIAMOJO PROCESO INFORMACINĖS SISTEMOS NAUDOTOJŲ ADMINISTRAVIMO TAISYKLĖS

I SKYRIUS BENDROSIOS NUOSTATOS

1. Integruotos baudžiamojo proceso informacinės sistemos naudotojų administravimo taisyklės (toliau – Naudotojų administravimo taisyklės) reglamentuoja Integruotos baudžiamojo proceso informacinės sistemos (toliau – IBPS) naudotojų ir administratorių teises ir pareigas, IBPS naudotojų administravimo principus ir tvarką, jų veiksmų kontrolę.

2. Naudotojų administravimo taisyklėse vartojamos sąvokos atitinka sąvokas, vartojamas 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“, 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), Integruotos baudžiamojo proceso informacinės sistemos duomenų saugos nuostatuose, patvirtintuose Lietuvos Respublikos vidaus reikalų ministro 2015 m. lapkričio 6 d. įsakymu Nr. 1V-876 „Dėl Integruotos baudžiamojo proceso informacinės sistemos duomenų saugos nuostatų patvirtinimo“ (toliau – Saugos nuostatai).

3. Naudotojų administravimo taisyklių reikalavimai taikomi visiems IBPS naudotojams, IBPS administratoriams – pagrindiniam IBPS administratoriui (administratoriams) ir IBPS tvarkytojų paskirtiems IBPS administratoriams, kuriems pagal Saugos nuostatų 14.3 papunktį suteikta teisė administruoti savo bei jiems pavaldžių įstaigų IBPS naudotojus, (toliau – IBPS tvarkytojo administratorius).

4. Kiekvienas IBPS naudotojas turi būti informacinėje sistemoje unikaliai identifikuojamas.

5. IBPS naudotojai turi turėti tik tiek prieigos teisių prie IBPS tvarkomos elektroninės informacijos, kiek tai būtina jų teisės aktų nustatytoms funkcijoms atlikti.

6. IBPS naudotojams prieiga prie IBPS suteikiama vadovaujantis principu „būtina žinoti“, kurio turinys apibrėžtas Vidaus reikalų informacinės sistemos centrinio duomenų banko naudotojų administravimo taisyklėse, patvirtintose Lietuvos Respublikos vidaus reikalų ministro 2008 m. gegužės 6 d. įsakymu Nr. 1V-165 „Dėl Vidaus reikalų informacinės sistemos centrinio duomenų banko naudotojų administravimo taisyklių patvirtinimo“ (toliau – VRIS naudotojų administravimo taisyklės).

II SKYRIUS

NAUDOTOJŲ IR ADMINISTRATORIŲ ĮGALIOJIMAI, TEISĖS IR PAREIGOS

7. IBPS naudotojai privalo užtikrinti IBPS elektroninės informacijos saugą ir tvarkyti IBPS elektroninę informaciją, vadovaudamiesi teisės aktais ir duomenų teikimo sutartimis.

8. IBPS naudotojai privalo saugoti IBPS tvarkomų asmens duomenų paslaptį Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymo nustatyta tvarka.

9. IBPS naudotojas turi tik tas prieigos prie IBPS teises, kurios buvo suteiktos Naudotojų administravimo taisyklių III skyriuje nustatyta tvarka.

10. IBPS naudotojai, pastebėję IBPS saugos dokumentuose nustatytų reikalavimų pažeidimų, nusikalstamos veikos požymių, neveikiančias arba netinkamai veikiančias saugos užtikrinimo priemones, privalo nedelsdami pranešti apie tai IBPS administratoriui, saugos įgaliotiniui arba:

10.1. pagrindinio IBPS administratoriaus (administratorių) administruojami IBPS naudotojai – Informatikos ir ryšių departamento Informacinių technologijų pagalbos tarnybai telefonu (8 5) 271 7777 arba elektroniniu paštu ittpagalba@vrm.lt;

10.2. Lietuvos Respublikos generalinės prokuratūros ir apygardų prokuratūrų IBPS naudotojai – elektroniniu paštu itsauga@prokuraturos.lt;

10.3. Nacionalinės teismų administracijos ir Lietuvos teismų IBPS naudotojai – it@teismai.lt.

11. IBPS naudotojams draudžiama:

11.1. atskleisti IBPS elektroninę informaciją ir suteikti kitokią galimybę bet kokia forma su ja susipažinti tokios teisės neturintiems asmenims;

11.2. savavališkai diegti IBPS taikomosios programinės įrangos pakeitimus ir naujas versijas neturint tam suteiktos teisės;

11.3. naudoti IBPS elektroninę informaciją kitokiais nei IBPS nuostatuose, kituose teisės aktuose ar duomenų teikimo sutartyje nurodytais tikslais;

11.4. sudaryti sąlygas pasinaudoti IBPS technine ir programine įranga tokios teisės neturintiems asmenims (paliekant darbo vietą, būtina užrakinti darbalaukį arba išjungti IBPS darbo stotį);

11.5. atlikti veiksmus, dėl kurių gali būti neteisėtai pakeisti ar sunaikinti IBPS duomenys;

11.6. atlikti bet kokius kitus neteisėtus IBPS tvarkymo veiksmus.

12. Pagrindinis IBPS administratorius (administratoriai) atlieka Saugos nuostatuose nurodytas funkcijas.

13. IBPS tvarkytojų administratoriai:

13.1. atlieka Saugos nuostatuose nurodytas funkcijas;

13.2. pagal kompetenciją teikia pagalbą ir konsultacijas IBPS naudotojams tvarkytojo įstaigoje bei tvarkytojo įstaigos reguliavimo ar veiklos sričiai priskirtose kitose įstaigose;

13.3. atlieka kitas IBPS saugos politiką įgyvendinančiuose dokumentuose, jų pareigybės aprašymuose ir kituose elektroninės informacijos saugą reglamentuojančiuose teisės aktuose nustatytas funkcijas.

14. Pagrindinis IBPS administratorius (administratoriai) administruoja tuos IBPS naudotojus, kurie nėra administruojami kitų IBPS tvarkytojų administratorių pagal šių Naudotojų administravimo taisyklių 16.2 punktą.

15. Sprendimas dėl teisės IBPS tvarkytojų administratoriams vadovaujantis Saugos nuostatų 14.3 papunkčiu, registruoti IBPS naudotojus ir suteikti jiems prieigos teisės priimamas per 5 darbo dienas nuo prašymo gavimo.

III SKYRIUS

SAUGAUS ELEKTRONINĖS INFORMACIJOS TEIKIMO IBPS NAUDOTOJAMS KONTROLĖS TVARKA

16. IBPS naudotojų įregistravimo ir išregistravimo tvarka:

16.1. IBPS naudotojai, kuriuos administruoja pagrindinis IBPS administratorius, administruojami *mutatis mutandis* VRIS naudotojų administravimo taisyklių nustatyta tvarka. Prašyme turi būti nurodyta, kokias prieigos teises prašoma suteikti IBPS naudotojui (vadovas, tyrėjas, dokumentų tvarkytojas, pataisos pareigūnas);

16.2. IBPS tvarkytojas, kurio paskirtam IBPS administratoriui šių Taisyklių 15 punkte nustatyta tvarka suteikta teisė administruoti IBPS naudotojus, juos administruoja vadovaudamasis savo valdomų valstybės informacinių išteklių, kurių technologinėmis priemonėmis administruojami IBPS naudotojai, naudotojų administravimo taisyklėmis. Lietuvos Respublikos generalinės prokuratūros ir apygardų prokuratūrų IBPS naudotojai administruojami vadovaujantis Informacinės prokuratūros sistemos naudotojų administravimo taisyklėmis, patvirtintomis Lietuvos Respublikos

generalinio prokuroro 2008 m. rugpjūčio 29 d. įsakymu Nr. I-114 „Dėl Informacinės prokuratūros sistemos saugos dokumentų patvirtinimo“. Nacionalinės teismų administracijos ir Lietuvos teismų IBPS naudotojai administruojami vadovaujantis Lietuvos teismų informacinės sistemos naudotojų administravimo taisyklėmis, patvirtintomis Nacionalinės teismų administracijos direktoriaus 2012 m. gruodžio 28 d. įsakymu Nr. 6P-151-(1.26) „Dėl Teisės aktų, reglamentuojančių Lietuvos teismų informacinėje sistemoje tvarkomų duomenų saugą, patvirtinimo“;

16.3. IBPS naudotojui pagrindinis IBPS administratorius arba IBPS tvarkytojo administratorius suteikia IBPS naudotojo vardą ir laikiną slaptažodį ir registruoja jį naudotojų administravimo posistemėje. Pagrindinis IBPS administratorius arba IBPS tvarkytojo administratorius prisijungimo duomenis perduoda asmeniškai arba išsiunčia tarnybiniu paštu IBPS naudotojui ne vėliau kaip per 5 darbo dienas nuo prašymo gavimo dienos;

16.4. kiekvienas IBPS naudotojas, jungdamasis prie IBPS, privalo atlikti tapatumo nustatymo procedūrą, t. y. nurodyti IBPS naudotojo vardą ir slaptažodį, kurį suteikė pagrindinis IBPS administratorius arba IBPS tvarkytojo administratorius;

16.5. kiekvienam IBPS naudotojui suteikiamas nesikartojantis vardas;

16.6. kiekvienas IBPS naudotojas privalo naudoti tik jam suteiktą IBPS naudotojo vardą; naudoti svetimą naudotojo vardą griežtai draudžiama;

16.7. IBPS tvarkytojų administratoriai visų jų administruojamų IBPS naudotojų duomenis ir jiems suteiktų prieigos teisių duomenis perduoda pagrindiniam IBPS administratoriui. Visų IBPS naudotojų ir jiems suteiktų prieigos teisių duomenys saugomi IBPS;

16.8. IBPS naudotojas suteiktą laikiną slaptažodį privalo pasikeisti pirmą kartą prisijungęs prie IBPS.

17. Reikalavimai IBPS naudotojų, IBPS administratorių slaptažodžiams, jų galiojimo trukmei, keitimui ir saugojimui:

17.1. pagrindinio IBPS administratoriaus arba IBPS tvarkytojo administratoriaus suteiktas laikinas slaptažodis IBPS naudotojui negali būti perduodamas atviru tekstu ar užšifruojamas nepatikimu algoritmu; IBPS saugos įgaliojimo sprendimu tik laikinas slaptažodis gali būti perduodamas atviru tekstu, tačiau atskirai nuo prisijungimo vardo, jei:

17.1.1. IBPS naudotojas neturi galimybių iššifruoti gauto užšifruoto slaptažodžio;

17.1.2. nėra techninių galimybių IBPS naudotojui perduoti slaptažodį šifruotu kanalu ar saugiu elektroninių ryšių tinklu.

17.2. IBPS naudotojas, IBPS administratorius, pirmą kartą jungdamasis prie IBPS, privalo pakeisti laikiną slaptažodį;

17.3. kilus įtarimui, kad slaptažodis galėjo būti atskleistas, IBPS naudotojas, IBPS administratorius turi nedelsdamas pakeisti slaptažodį;

- 17.4. pasirinkdamas ar keisdamas slaptažodį, IBPS naudotojas, IBPS administratorius turi bent kartą slaptažodį pakartoti;
- 17.5. draudžiama naudoti anksčiau to paties IBPS naudotojo naudotus slaptažodžius;
- 17.6. slaptažodžiai IBPS saugomi naudojant maišos funkcijas;
- 17.7. IBPS naudotojas, IBPS administratorius slaptažodį turi įsiminti. Draudžiama slaptažodį užsirašyti ar atskleisti kitam asmeniui;
- 17.8. didžiausias leistinas mėginimų įvesti teisingą slaptažodį skaičius yra 5 kartai; slaptažodį, neteisingai įvedus didžiausią leistiną skaičių, IBPS užsirakina ir neleidžia IBPS naudotojui identifikuotis 15 minučių;
- 17.9. papildomi reikalavimai IBPS naudotojo slaptažodžiams:
 - 17.9.1. slaptažodis sudaromas iš ne mažiau kaip 8 simbolių;
 - 17.9.2. slaptažodis sudaromas iš raidžių, skaičių ir specialiųjų simbolių;
 - 17.9.3. slaptažodis keičiamas kas 3 mėnesius. IBPS naudotojo teisės sustabdomos, jei slaptažodis nepakeičiamas laiku;
 - 17.9.4. keičiant slaptažodį, neleidžiama sudaryti slaptažodžio iš buvusių 6 paskutinių slaptažodžių;
- 17.10. papildomi reikalavimai IBPS administratorių slaptažodžiams:
 - 17.10.1. slaptažodis keičiamas ne rečiau kaip kas 2 mėnesius;
 - 17.10.2. slaptažodis sudaromas iš ne mažiau kaip 12 simbolių;
 - 17.10.3. keičiant slaptažodį, neleidžiama sudaryti slaptažodžio iš buvusių 3 paskutinių slaptažodžių.
18. IBPS naudotojų teisių dirbti su IBPS elektronine informacija sustabdymo atvejai:
 - 18.1. kai IBPS naudotojas, IBPS administratorius nesinaudoja IBPS ilgiau kaip 3 mėnesius;
 - 18.2. įstatymų nustatytais atvejais IBPS naudotojas, IBPS administratorius nušalinamas nuo darbo (pareigų).
19. IBPS naudotojo teisė dirbti su IBPS elektronine informacija panaikinama:
 - 19.1. jei IBPS naudotojas nustoja vykdyti funkcijas, kurių vykdymui buvo suteiktos prieigos prie IBPS teisės;
 - 19.2. nustačius IBPS elektroninės informacijos konfidencialumo ar vientisumo pažeidimą arba kitų IBPS elektroninės informacijos ir IBPS informacijos saugą ir tvarkymą reglamentuojančių teisės aktų ar IBPS duomenų teikimo sutarties nustatytų reikalavimų pažeidimą;
 - 19.3. pasibaigus IBPS naudotojo tarnybos (darbo) santykiams.
20. Nuotolinio prisijungimo būdu prie IBPS jungiamasi per virtualųjį privatų tinklą (VPN) naudojant šifruotą kanalą.

21. IBPS naudotojai gali jungtis prie IBPS naudodamiesi mobiliojo ryšio operatorių teikiamomis paslaugomis. Tokiu atveju galiniams įrenginiams ir duomenų perdavimui taikomos papildomos saugumo priemonės (duomenų šifravimas, perdavimo kanalo „tuneliai“ ir kitos saugos priemonės).

22. Techninės nuotolinių prisijungimų prie IBPS sąlygos nustatomos Nuotolinio prisijungimo prie Vidaus reikalų informacinės sistemos centrinio duomenų banko tvarkos apraše, patvirtintame Lietuvos Respublikos vidaus reikalų ministro 2012 m. gruodžio 11 d. įsakymu Nr. 1V-904 „Dėl Nuotolinio prisijungimo prie Vidaus reikalų informacinės sistemos centrinio duomenų banko tvarkos aprašo patvirtinimo“.

23. Nuotolinį prisijungimą prie IBPS naudojančiam IBPS naudotojui draudžiama savavališkai diegti technines ir programines priemones į nuotoliniam prisijungimui naudojamą įrangą bei daryti kitokius jos pakeitimus.

IV SKYRIUS BAIGIAMOSIOS NUOSTATOS

24. IBPS naudotojai, IBPS administratoriai pažeidę Naudotojų administravimo taisyklių nuostatas, atsako įstatymų nustatyta tvarka.
