(2025 m. birželio 4 d. įsakymo Nr. BR1-207 redakcija nuo 2025 m. birželio 4 d.)

Nacionalinės mokėjimo agentūros
prie Žemės ūkio ministerijos
informacijos saugumo politikos
4 priedas

NACIONALINĖS MOKĖJIMO AGENTŪROS PRIE ŽEMĖS ŪKIO MINISTERIJOS INFORMACIJOS SAUGUMO POLITIKOS SANTRAUKA

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Nacionalinės mokėjimo agentūros prie Žemės ūkio ministerijos informacijos saugumo politika (toliau – Informacijos saugumo politika) – tai dokumentas, reglamentuojantis pagrindines Nacionalinės mokėjimo agentūros prie Žemės ūkio ministerijos informacijos saugumo nuostatas.

2. Informacijos saugumo politiką įsakymu tvirtina Nacionalinės mokėjimo agentūros prie Žemės ūkio ministerijos direktorius. Šio dokumento dalys gali būti išplatinamos su Nacionalinės mokėjimo agentūros prie Žemės ūkio ministerijos informacija susijusioms šalims joms prieinama ir suprantama forma.

3. Informacijos saugumo politikos tikslas – pateikti Nacionalinės mokėjimo agentūros prie Žemės ūkio ministerijos vadovybės poziciją informacijos saugumo atžvilgiu.

4. Informacija – tai strategiškai svarbus Nacionalinės mokėjimo agentūros prie Žemės ūkio ministerijos veiklai turtas, todėl jos praradimas, neteisėtas pakeitimas, sugadinimas ar informacijos apdorojimo nutraukimas gali sukelti Nacionalinės mokėjimo agentūros prie Žemės ūkio ministerijos veiklos sutrikimų. Atsižvelgiant į tai, ši Informacijos saugumo politika nustato pagrindines gaires, kuriomis, siekiant apsaugoti Nacionalinės mokėjimo agentūros prie Žemės ūkio ministerijos informaciją, privalo vadovautis visi Nacionalinės mokėjimo agentūros prie Žemės ūkio ministerijos valstybės tarnautojai ir darbuotojai, dirbantys pagal darbo sutartis, rangovai, susijusios šalys. Informacijos saugumo politiką tvirtina Nacionalinės mokėjimo agentūros prie Žemės ūkio ministerijos vadovybė.

5. ***(2018 m. birželio 1 d. įsakymo Nr. BR1-141 redakcija nuo 2018 m. birželio 1 d.)***

Informacijos saugumo politika taikoma visiems Nacionalinės mokėjimo agentūros prie Žemės ūkio ministerijos veiklos procesams ir apima žodinę bei rašytinę informaciją, informacines sistemas, kompiuterių tinklus, fizinę aplinką, valstybės tarnautojus ir darbuotojus, dirbančius pagal darbo sutartis, susijusias šalis, rangovus, įskaitant dirbančius nuotoliniu būdu ar kitus Nacionalinėje mokėjimo agentūroje prie Žemės ūkio ministerijos dirbančius asmenis, įskaitant darbuotojus, dirbančius trečiosioms šalims, teisėtai tvarkančius Nacionalinės mokėjimo agentūros prie Žemės ūkio ministerijos informaciją.

6. Informacijos saugumas apima tris pagrindinius aspektus:

6.1. informacijos konfidencialumas – informacijos apsauga nuo nesankcionuoto paskelbimo;

6.2. vientisumas – informacijos apsauga nuo nesankcionuoto ar atsitiktinio pakeitimo;

6.3. prieinamumas – užtikrinimas, kad informacija yra prieinama tada, kai ji reikalinga tinkamai vykdyti Nacionalinės mokėjimo agentūros prie Žemės ūkio ministerijos veiklą.

7. Informacijos saugumo politika:

7.1. aprašo Nacionalinės mokėjimo agentūros prie Žemės ūkio ministerijos politiką, skirtą apsaugoti jos informacinio turto, t. y. techninės įrangos, programinės įrangos, patalpų ir informacijos, konfidencialumą, vientisumą ir prieinamumą;

7.2. nustato atsakomybę už informacijos saugumą;

7.3. pateikia nuorodas į saugumo dokumentus, kurie sudaro informacijos saugumo valdymo sistemą.

8. Informacijos saugumo politikos santrauka turi būti peržiūrima ne rečiau kaip kartą per metus.

II SKYRIUS
SĄVOKOS IR SUTRUMPINIMAI

9. Šioje Informacijos saugumo politikos santraukoje vartojamos sąvokos:

9.1. ***(2020 m. liepos 23 d. įsakymo Nr. BR1-280 redakcija nuo 2020 m. rugpjūčio 1 d.)***

Duomenų apsaugos pareigūnas – Nacionalinės mokėjimo agentūros prie Žemės ūkio ministerijos direktoriaus įsakymu paskirtas Prevencijos ir saugos departamento Informacijos saugos skyriaus valstybės tarnautojas ar darbuotojas, dirbantis pagal darbo sutartį, atliekantis duomenų apsaugos pareigūno funkcijas;

9.2. **Informacijos saugumas** – apima informacijos konfidencialumo, vientisumo ir prieinamumo išsaugojimą. Papildomai gali būti įtraukti ir kiti kriterijai, tokie kaip autentiškumas, atskaitingumas, neišsižadėjimas ir patikimumas;

9.3. ***(2018 m. gegužės 8 d. įsakymo Nr. BR1-117 redakcija nuo 2018 m. gegužės 8 d.)***

Informacijos saugumo incidentas – vienas ar daugiau nepageidaujamų ir netikėtų informacijos saugumo įvykių, turinčių didelę tikimybę pakenkti veiklai ir keliančių grėsmę informacijos saugumui;

9.4. ***(2018 m. gegužės 8 d. įsakymo Nr. BR1-117 redakcija nuo 2018 m. gegužės 8 d.)***

Informacijos saugumo įvykis – nustatytas sistemos, tarnybos ar tinklo įvykis, rodantis galimą informacijos saugumo politikos spragą ar informacijos saugumo priemonių triktį arba anksčiau nenumatytos situacijos, kuri gali būti susijusi su informacijos saugumu, atsiradimą;

9.5. ***(2020 m. liepos 23 d. įsakymo Nr. BR1-280 redakcija nuo 2020 m. rugpjūčio 1 d.)***

Informacijos saugos įgaliotinis – Nacionalinės mokėjimo agentūros prie Žemės ūkio ministerijos direktoriaus įsakymu paskirtas Prevencijos ir saugos departamento Informacijos saugos skyriaus valstybės tarnautojas ar darbuotojas, dirbantis pagal darbo sutartį, atsakingas už informacijos saugumo valdymo Nacionalinėje mokėjimo agentūroje prie Žemės ūkio ministerijos įgyvendinimą ir palaikymą;

9.6. **Kenksminga programinė įranga –** programinė įranga, turinti kenkėjiškų tikslų ar daranti neigiamą įtaką, pvz.: virusai, „kirminai“, „Trojos arkliai“, šnipinėjimo programinė įranga ir pan.;

9.7. **Konfidenciali informacija –** informacija, prieinama ir atskleidžiama tik įgaliotiems asmenims;

9.8. **Konfidencialumas** – savybė, nusakanti tai, kad informacija nebus prieinama ar pateikiama neįgaliotiems fiziniams ar juridiniams asmenims arba procesams;

9.9. **Naudotojas** – Nacionalinės mokėjimo agentūros prie Žemės ūkio ministerijos valstybės tarnautojas ar darbuotojas, dirbantis pagal darbo sutartį, rangovas, laikinai dirbantis konsultantas ar kitas Nacionalinėje mokėjimo agentūroje prie Žemės ūkio ministerijos dirbantis asmuo, įskaitant darbuotojus, dirbančius trečiosioms šalims, teisėtai tvarkančius Nacionalinės mokėjimo agentūros prie Žemės ūkio ministerijos informaciją, kuriems suteikta priėjimo prie Nacionalinės mokėjimo agentūros prie Žemės ūkio ministerijos informacijos ir (ar) informacinių sistemų teisė naudotis informacinės sistemos ištekliais numatytoms funkcijoms atlikti;

9.10. **Programinė įranga** – taikomoji programinė įranga, sisteminė programinė įranga, plėtros priemonės ir paslaugų programos;

9.10[1]. ***(2025 m. birželio 4 d. įsakymo Nr. BR1-207 redakcija nuo 2025 m. birželio 4 d.)***

Galinis įrenginys – informacijai priimti ir (arba) perduoti skirtas įrenginys ar jo dalis, kurie tiesiogiai ar netiesiogiai bet kokiomis priemonėmis yra prijungiami prie NMA vidinių elektroninių ryšių tinklų;

9.11. **Šifravimas –** duomenų pakeitimo procesas iš pradinės būsenos į būseną, kai duomenys negali būti perskaityti (naudojami) neturint priemonių / informacijos (šifravimo rakto), kuriomis galima duomenis sugrąžinti į pradinę būseną;

9.12. **Trečiasis asmuo** – asmuo ar organizacija, kuri pripažįstama nepriklausoma nuo dalyvaujančių asmenų, nagrinėjant svarstomą klausimą;

9.13. **Turtas** – visa, kas turi kokią nors vertę Nacionalinei mokėjimo agentūrai prie Žemės ūkio ministerijos. Nacionalinės mokėjimo agentūros prie Žemės ūkio ministerijos vadybos sistemų vadovo, patvirtinto Nacionalinės mokėjimo agentūros prie Žemės ūkio ministerijos direktoriaus 2013 m. gruodžio 30 d. įsakymu Nr. BR1-1404 „Dėl Nacionalinės mokėjimo agentūros prie Žemės ūkio ministerijos vadybos sistemų vadovo patvirtinimo“, 11 priede „Informacijos saugumo rizikos valdymo tvarkos aprašas“ turtas apibrėžiamas kaip informaciniai ištekliai;

9.14. ***(2024 m. sausio 22 d. įsakymo Nr. BR1- 17 redakcija nuo 2024 m. sausio 22 d.)***

Vadovybė – Nacionalinės mokėjimo agentūros prie Žemės ūkio ministerijos direktorius, direktoriaus pavaduotojai.

10. Šioje Informacijos saugumo politikos santraukoje vartojami sutrumpinimai:

10.1. **Agentūra** – Nacionalinė mokėjimo agentūra prie Žemės ūkio ministerijos;

10.2. **ES –** Europos Sąjunga;

10.3. **IT** – informacinės technologijos;

10.4. **Tarnautojai** – Agentūros valstybės tarnautojai ir darbuotojai, dirbantys pagal darbo sutartis.

III SKYRIUS
INFORMACIJOS SAUGUMO ORGANIZAVIMAS

11. Vadovybė užtikrina Agentūros Informacijos saugumą, aiškiai vadovaudama šiam procesui, prisiimdama įsipareigojimus bei aiškiai paskirstydama atsakomybę už Informacijos saugumą.

12. Susijusių šalių, rangovų atstovai privalo:

12.1. laikytis Agentūros Informacijos saugumo politikos ir susijusių dokumentų reikalavimų;

12.2. ***(2025 m. birželio 4 d. įsakymo Nr. BR1-207 redakcija nuo 2025 m. birželio 4 d.)***

saugoti jiems patikėtą Agentūros techninę įrangą, Programinę įrangą, galinius įrenginius ir informaciją;

12.3. neleisti įdiegti Kenksmingos programinės įrangos į Agentūros informacines sistemas;

12.4. pagal nustatytą tvarką pranešti apie visus įtariamus ar įvykusius Informacijos saugumo įvykius;

12.5. informuoti Agentūrą tą pačią dieną, kurią sužinoma, kad atleidžiamas rangovo darbuotojas, turintis prieigos prie Agentūros informacijos ar informacinių sistemų teises, bet ne vėliau kaip rangovo darbuotojo atleidimo dieną.

IV SKYRIUS
INFORMACINĖS SISTEMOS NAUDOJIMO TAISYKLĖS

13. Informacinės sistemos naudojimo taisyklių tikslas – apsaugoti Agentūrą, jos Tarnautojus, partnerius nuo tyčia ar netyčia asmenų atliktų neteisėtų ir (arba) kenksmingų veiksmų, ir jų sukeltų padarinių. Šios taisyklės (toliau – Naudotojo standartas) nustato informacinių ir

komunikacinių technologijų priimtino naudojimo darbo vietoje darbo metu taisykles, taip pat Naudotojų stebėsenos ir kontrolės darbo vietoje taisykles bei mastą.

14. ***(2025 m. birželio 4 d. įsakymo Nr. BR1-207 redakcija nuo 2025 m. birželio 4 d.)***

Agentūros informacinė sistema, įskaitant (bet neapsiribojant) elektroninę informaciją, internetą, intranetą, vidinį kompiuterių tinklą, techninę įrangą (tarnybinės stotys, galiniai įrenginiai), operacines sistemas, duomenų laikmenas, informacinės sistemos sąskaitas, elektroninį paštą, naršymą internete (toliau – Informacinė sistema), yra Agentūros nuosavybė.

15. Informacinė sistema turi būti naudojama tik veiklos funkcijoms atlikti.

16. Agentūros Informacijos saugumas priklauso nuo visų Tarnautojų bei susijusių trečiųjų šalių, kurios vienaip ar kitaip naudojasi Agentūros informacija, pastangų, todėl kiekvienas Naudotojas privalo susipažinti su šiuo Naudotojo standartu bei elgtis, kaip jame apibrėžta.

17. Šio Naudotojo standarto nuostatos privalomos visiems Naudotojams.

18. Bendri informacinės sistemos naudojimo principai:

18.1. Naudotojai privalo Informacinę sistemą naudoti tik darbo reikmėms pagal patvirtintas darbo procedūras ir Informacinės sistemos naudotojo instrukcijas;

18.2. Informacijos saugumo ir Informacinės sistemos priežiūros tikslais įgalioti Tarnautojai gali bet kuriuo metu tikrinti techninės ar Programinės įrangos darbą, kompiuterių tinklo srautą ir Naudotojų veiksmus Informacinėje sistemoje;

18.3. Agentūra, siekdama užtikrinti Naudotojo standarto reikalavimų laikymąsi, pasilieka teisę audituoti Informacinę sistemą ir joje atliekamus veiksmus;

18.4. Naudotojai turi teisę konsultuotis su Informacinių technologijų departamento Tarnautojais techninės ir Programinės įrangos eksploatavimo klausimais;

18.5. Naudotojai privalo saugoti Informacinės sistemos slaptažodžius. Draudžiama keistis prisijungimo prie Informacinės sistemos vardais, prisijungti prie Informacinės sistemos pasinaudojus kito Naudotojo prisijungimo duomenimis;

18.6. jokiomis aplinkybėmis Naudotojai, naudodami Informacinę sistemą, negali vykdyti veiklos, kuri yra nelegali ar nusikalstama ar kitaip pažeidžia Lietuvos Respublikos ar tarptautinius teisės aktus;

18.7. ***(2018 m. birželio 1 d. įsakymo Nr. BR1-141 redakcija nuo 2018 m. birželio 1 d.)***

ES ir Lietuvos Respublikos teisės aktų, reglamentuojančių asmens duomenų apsaugą, klausimais Naudotojus konsultuoja ir rekomendacijas teikia duomenų apsaugos pareigūnas, kurio kontaktiniai duomenys yra skelbiami viešai interneto svetainės www.nma.lt skiltyje „Asmens duomenų apsauga“.

19. Žemiau išvardinti veiksmai yra draudžiami. Gali būti taikomos išimtys tiems Naudotojams, kuriems nurodyti veiksmai yra būtini atliekant teisėtas veiklos funkcijas (pvz.: Informacinės sistemos priežiūra, Informacijos saugumo incidentų tyrimas ir pan.). Žemiau pateiktas draudžiamų veiksmų sąrašas nėra baigtinis, jis yra daugiau informacinio pobūdžio, leidžiantis Naudotojui suvokti galimai neleistinų veiksmų ribas:

19.1. skelbti Agentūros Konfidencialią informaciją internete;

19.2. pažeisti asmenų teises, kurios saugomos prekės ženklų, komercinių paslapčių, patentų ar kitų intelektualios nuosavybės ar kitų susijusių teisių, įskaitant (bet neapsiribojant) nelegalios Programinės įrangos (ar kitos Programinės įrangos, kurios naudojimo teisės Agentūra neturi) diegimą, saugojimą, naudojimą, kopijavimą ar platinimą;

19.3. neleistinai kopijuoti autorių teisių saugomą turinį, įskaitant (bet neapsiribojant) vaizdų ar teksto skenavimą tiek dalimis, tiek ištisai iš knygų, žurnalų ar kitų šaltinių, muzikos įrašų, Programinės įrangos ir pan. kopijavimą;

19.4. eksportuoti Programinę ar techninę įrangą, Šifravimo technologijas ar Šifravimo būdus, pažeidžiant Lietuvos Respublikos ar ES eksporto ribojimo reikalavimus (kilus abejonių būtina pasikonsultuoti su Informacijos saugos įgaliotiniu);

19.5. parsisiųsti arba platinti tiesiogiai su darbu nesusijusią grafinę, garso ir vaizdo medžiagą, žaidimus ir Programinę įrangą, siųsti duomenis, kurie yra užkrėsti virusais, turi įvairius kitus žalingus programinius kodus, bylas, galinčias sutrikdyti kompiuterinių ar telekomunikacinių įrenginių bei Programinės įrangos funkcionavimą ir saugumą;

19.6. ***(2025 m. birželio 4 d. įsakymo Nr. BR1-207 redakcija nuo 2025 m. birželio 4 d.)*** savarankiškai keisti ir taisyti Galinius įrenginius (IT ir telekomunikacijų techninę) ir Programinę įrangą;

19.7. atskleisti prisijungimo prie Informacinės sistemos duomenis kitiems asmenims (įskaitant šeimos narius, jei dirbama namuose);

19.8. naudoti Informacinę sistemą teisės aktais draudžiamai veiklai, šmeižiančio, įžeidžiančio, grasinamojo pobūdžio ar visuomenės dorovės ir moralės principams prieštaraujančiai informacijai, kompiuterių virusams, masinei piktybiškai informacijai (angl. *spam*) siųsti ar kitiems tikslams, kurie gali pažeisti Agentūros ar kitų asmenų teisėtus interesus;

19.9. naudoti Informacinę sistemą kuriant ar perduodant žiauraus, įžeidžiančio, pornografinio ar panašaus turinio informaciją arba informaciją, kurią galima traktuoti kaip seksualinį priekabiavimą;

19.10. bet kokia forma diskriminuoti ar priekabiauti naudojantis el. paštu, telefonu ar bet kokia kita forma, pavyzdžiui pranešimų dažnumu, dydžiu ar pan.;

19.11. naudoti elektroninį paštą ir interneto prieigą asmeniniams, komerciniams tikslams, siūlyti ne Agentūros teikiamas prekes ar paslaugas, naudojantis Agentūros vardu;

19.12. ***(2025 m. birželio 4 d. įsakymo Nr. BR1-207 redakcija nuo 2025 m. birželio 4 d.)*** naudoti Programinę įrangą ir (arba) galinius įrenginius neteisėtai prieigai prie Informacinės sistemos ar jos duomenų saugumo tikrinimui, skenavimui, kompiuterinio tinklo srauto duomenų stebėjimui;

19.13. rinkti kompiuterių tinklu perduodamus duomenis ar jų fragmentus, analizuoti jų pobūdį, kiekį ar pan., nebent tai būtina atliekant teisėtas veiklos funkcijas (pvz.: Informacinės sistemos priežiūra, Informacijos saugumo incidentų tyrimas ir pan.);

19.14. bandyti apeiti Naudotojo prieigos prie Informacinės sistemos tapatybės nustatymo mechanizmus;

19.15. vykdyti paslaugos atsisakymo atakas ar kitaip trukdyti kitų Naudotojų darbą Informacinėje sistemoje;

19.16. ***(2025 m. birželio 4 d. įsakymo Nr. BR1-207 redakcija nuo 2025 m. birželio 4 d.)*** perduoti Agentūrai priklausančius galinius įrenginius (IT ir telekomunikacijų techninę) ir Programinę įrangą Tretiesiems asmenims, jei toks perdavimas nėra susijęs su darbinių funkcijų vykdymu ar gali bet kokiu būdu pakenkti Agentūros interesams;

19.17. teikti informaciją apie Naudotojus ar teikti Naudotojų sąrašus ne Tarnautojams;

19.18. išnaudoti Informacinės sistemos Pažeidžiamumus, įskaitant (bet neapsiribojant) prieigą prie duomenų, kurie neskirti Naudotojui prisijungti prie Informacinės sistemos ar jos dalies, nebent tai būtina atliekant teisėtas veiklos funkcijas (pvz.: Informacinės sistemos priežiūra, Informacijos saugumo incidentų tyrimas ir pan.);

19.19. keisti ar kitaip neleistinai naudoti el. pašto aprašą (angl. *header*);

19.20. naudoti kito Naudotojo el. pašto adresą;

19.21. kurti ar persiųsti grandininius el. laiškus, kuriuose skatinama persiųsti el. laišką savo draugams ar pan.;

19.22. atlikti kitus su darbo funkcijų vykdymu nesusijusius ar teisės aktams prieštaraujančius veiksmus.

20. Taip pat, negavus Agentūros direktoriaus arba jo įgaliotų Tarnautojų patvirtinimo, draudžiama siųsti elektroniniu paštu informaciją apie Informacinės sistemos funkcionavimo principus ir jų reglamentavimą, Informacijos saugumo užtikrinimo bei kontrolės priemones.

21. Naudotojams naudojant elektroninio pašto ir interneto resursus asmeniniais tikslais, Agentūra neužtikrina asmeninės informacijos Konfidencialumo.

22. Atpažinimas ir tapatybės patvirtinimas. Naudotojas privalo:

22.1. laikytis nustatytų slaptažodžio naudojimo sąlygų:

22.1.1. laikyti slaptažodį paslaptyje ir neperduoti jo jokiam asmeniui bet kokiomis sąlygomis;

22.1.2. ***(2021 m. kovo 25 d. įsakymo Nr. BR1-100 redakcija nuo 2021 m. kovo 25 d.)***

pakeisti slaptažodį ne rečiau kaip kartą per 2 mėnesius (šis reikalavimas be išimčių taikomas ir administratoriams);

22.1.3. naudoti slaptažodį, turintį mažiausiai 8 ženklus;

22.1.4. naudoti unikalų slaptažodį, kurio negalima pakartotinai naudoti iš tokių pat slaptažodžių kaip buvę 6 paskutiniai slaptažodžiai;

22.1.5. naudoti slaptažodį, sudarytą iš raidžių, skaičių ir specialių simbolių;

22.1.6. sudarant slaptažodį nenaudoti asmeninio pobūdžio informacijos, plačiai žinomų žodžių ir pavadinimų (pvz., Vilnius).

22.2. laikytis Informacinės sistemos administratoriams nustatytų papildomų slaptažodžio naudojimo sąlygų:

22.2.1. ***(2021 m. kovo 25 d. įsakymo Nr. BR1-100 redakcija nuo 2021 m. kovo 25 d.)***

Neteko galios

22.2.2. naudoti slaptažodį, kurį sudaro mažiausiai 12 ženklų;

22.2.3. pakartotinai nenaudoti tokio pat slaptažodžio kaip buvę 3 paskutiniai slaptažodžiai;

22.2.4. saugoti slaptažodį seife;

22.2.5. ***(2022 m. gruodžio 30 d. įsakymo Nr. BR1-449 redakcija nuo 2022 m. gruodžio 30 d.)***

jei slaptažodžiai saugomi elektroninėje laikmenoje, ji turi būti užšifruojama su slaptažodžiu.

23. Naudotojo prieiga prie Informacinės sistemos yra blokuojama, kai slaptažodis 3 kartus iš eilės įvedamas klaidingai. Tokiu atveju Naudotojas privalo kreiptis į Agentūros Pagalbos tarnybą ir pakartotinai prisijungti prie Informacinės sistemos tik administratoriui leidus.

24. Naudotojas, be Informacinių technologijų departamento Sistemų administravimo skyriaus Tarnautojo leidimo, privalo susilaikyti nuo:

24.1. bet kokių programų, gautų iš interneto ar pateiktų diskuose ar kitokiomis formomis, diegimo ir neleistino naudojimo;

24.2. kompiuterio techninės įrangos ir operacinės sistemos konfigūracijos keitimo;

24.3. nelicencijuotos ir nesankcionuotos Programinės įrangos naudojimo.

25. Naudotojas privalo užtikrinti Konfidencialios informacijos naudojimą ir tvarkymą taip kaip numatyta sutarties sąlygose.

26. ***(2025 m. birželio 4 d. įsakymo Nr. BR1-207 redakcija nuo 2025 m. birželio 4 d.)***

Naudotojas, pastebėjęs Informacinės sistemos veikimo sutrikimų, privalo apie juos nedelsdamas pranešti Agentūros Pagalbos tarnybai (el. paštu pagalba@nma.lt arba telefonu +370 5 252 688) ir už sutartį atsakingam Tarnautojui (jei santykiai pagrįsti Agentūros ir trečiosios šalies sutartimi). Apie Informacijos saugumo įvykį Naudotojas nedelsdamas privalo informuoti Informacijos saugos įgaliotinį (el. paštu saugos.igaliotinis@nma.lt arba telefonu +370 5 252 6909) bei savo tiesioginį vadovą.

27. Susijusių šalių ir rangovų atstovų atsakomybė už visų informacijos apdorojimo išteklių naudojimą tiek tais atvejais, kai šiais ištekliais naudojasi jie patys, tiek tais atvejais, kai šiais ištekliais naudojasi kiti jų įgalioti asmenys numatoma sutartyse.

28. Agentūra, siekdama apsaugoti: Agentūros Konfidencialią informaciją, klientų ir Naudotojų asmens duomenis nuo atskleidimo Tretiesiems asmenims; Informacinę sistemą nuo kibernetinių atakų, įsilaužimų ir duomenų vagysčių, virusų, pavojingų interneto puslapių, Kenksmingos programinės įrangos; Agentūros Turtą ir užtikrinti saugumą Agentūros patalpose bei

teritorijoje; Agentūros interesus ir užtikrinti darbo pareigų ir vidaus tvarkos laikymąsi, ir vadovaudamasi būtinumo, tikslingumo, skaidrumo, proporcingumo, tikslumo ir duomenų išsaugojimo bei saugumo principais, tiek ir tokia apimtimi, kiek tai yra būtina numatytiems tikslams pasiekti, atlieka Naudotojų stebėseną ir kontrolę darbo vietoje.

_____