Suvestinė redakcija nuo 2024-11-08

PATVIRTINTA
Vilniaus universiteto rektoriaus
2021 m. gruodžio 20 d. įsakymu Nr. R-440
(Vilniaus universiteto rektoriaus
2024 m. vasario 8 d. įsakymo Nr. R-82
redakcija)

VILNIAUS UNIVERSITETO INFORMACINIŲ IŠTEKLIŲ NAUDOTOJŲ ADMINISTRAVIMO TAISYKLĖS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Vilniaus universiteto informacinių išteklių naudotojų administravimo taisyklės (toliau – Taisyklės) reglamentuoja Vilniaus universiteto (toliau – Universitetas) centralizuotai valdomų arba autentifikuojamų informacinių išteklių naudotojų, naudotojų teisių administratorių ir kitų administratorių bei įgaliotų asmenų teises, pareigas, prieigos prie studijų ir vidaus administravimo tikslais naudojamų Universiteto informacinių išteklių administravimo principus, saugaus elektroninės informacijos teikimo naudotojams tvarką.

2. Universiteto padaliniai, atsakingi už valstybės informacinių sistemų, atviros prieigos ir kitus, nei 1 punkte nurodyti, Universiteto informacinius išteklius, vadovaujasi šiomis Taisyklėmis arba, vadovaudamiesi šiomis Taisyklėmis ir nurodytais teisės aktais, parengia jų administruojamiems informaciniams ištekliams skirtas naudotojų administravimo taisykles.

3. Taisyklės parengtos vadovaujantis Bendrųjų elektroninės informacijos saugos reikalavimų aprašu, patvirtintu Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo ir Saugos dokumentų turinio gairių aprašo patvirtinimo“ (toliau – Bendrųjų elektroninės informacijos saugos reikalavimų aprašas), Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašu, patvirtintu Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“ (toliau – Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašas), taip pat kitais teisės aktais ir standartais, reglamentuojančiais duomenų tvarkymo teisėtumą, tvarkytojų veiklą ir duomenų saugos valdymą.

4. Šiose Taisyklėse naudojamos sąvokos:

4.1. **Informacinių išteklių naudotojas** (toliau – naudotojas) – Universiteto informacinių išteklių prieigos administravimo funkcijų neatliekantis, sutartiniais ar kitais teisės aktuose ar kituose Universiteto dokumentuose numatytais teisėtais pagrindais naudojantis priskirtus Universiteto informacinius išteklius asmuo;

4.2. **Įgaliotas asmuo** – Universiteto kamieninio ar jo šakinio padalinio, įgyvendinančio Universiteto informacinio ištekliaus valdymą (toliau – padalinys, įgyvendinantis Universiteto informacinio ištekliaus valdymą), vadovas ar jo paskirtas darbuotojas, duomenų valdymo įgaliotinis, duomenų apsaugos pareigūnas, informacijos saugos vadovas ar darbuotojo tiesioginis vadovas, galintis nurodyti naudotojui, naudotojų teisių administratoriui ar kitam administratoriui atlikti papildomus veiksmus dėl paskyrų ir prieigos teisių tvarkymo;

4.3. **Naudotojų teisių administratorius** – padalinio, įgyvendinančio Universiteto informacinio ištekliaus valdymą, vadovo paskirtas darbuotojas arba Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymo 41 straipsnyje nurodyti paslaugos teikėjo darbuotojas, vykdantis Universiteto informacinio ištekliaus prieigos teisių naudotojams tvarkymą, naudotojų teisių administravimą, vadovaujantis šiose Taisyklės nurodytais principais, ir kitas šiose Taisyklėse nustatytas funkcijas;

4.4. **Paskyra** – naudotojo asmens duomenų, būtinų nustatant naudotojo tapatybę, ir prieigos teisių prie Universiteto informacinių išteklių registravimo duomenų rinkinys;

4.5. **Universiteto informaciniai ištekliai** – informacijos, kurią valdo Universitetas, atlikdamas savo funkcijas, apdorojamos informacinių technologijų priemonėmis (sistemine ir tinklo įranga, programomis, moduliais ir kita), ir ją apdorojančių informacinių sistemų ir vidaus registrų visuma;

4.6. **Universiteto informacinių išteklių valdymas** – Universiteto informacinių išteklių kūrimo, tvarkymo, plėtros tikslų nustatymas, jų tvarkymo ir priežiūros organizavimas ir kontrolė, darbuotojų, informacinių technologijų priemonėmis apdorojančių informaciją, dokumentus ir (arba) jų kopijas, veiklos organizavimas ir priežiūra.

4.7. Kitos Taisyklėse naudojamos sąvokos suprantamos taip, kaip apibrėžtos Bendrųjų elektroninės informacijos saugos reikalavimų apraše ir kituose informacinius išteklius reglamentuojančiuose teisės aktuose bei saugų duomenų tvarkymą reglamentuojančiuose standartuose.

5. Taisyklės privalomos visiems Taisyklių 1 punkte nurodytų Universiteto informacinių išteklių naudotojams bei administratoriams.

6. Prieiga prie Universiteto informacinių išteklių suteikiama vadovaujantis šiais principais:

6.1. prieiga suteikiama tik teisėtais pagrindais;

6.2. prieiga suteikiama tik atlikus naudotojo identifikaciją ir patvirtinus jo tapatybę;

6.3. prieiga keisti (sukurti, papildyti ar panaikinti) duomenis turi būti suteikiama tik prie tų Universiteto informacinių išteklių, kurie būtini naudotojo funkcijoms atlikti;

6.4. naudotojų teisių administratoriaus funkcijos turi būti atliekamos naudojant atskirą tam skirtą paskyrą, kuria naudojantis draudžiama atlikti naudotojo funkcijas. Kai galimybė atskirti naudotojų teisių administratorių ir naudotojų funkcijas nėra įgyvendinta informacinio ištekliaus priemonėmis, pakeitimus leidžiama atlikti tik suderinus su šių Taisyklių įgyvendinimą užtikrinti įgaliotu asmeniu.

7. Teisės naudoti Universiteto informacinius išteklius suteikiamos tik susipažinus su šių Taisyklių reikalavimais ir atsakomybe už jų nesilaikymą bei įsipareigojus jų laikytis. Įsipareigojimai patvirtinami elektroniniu būdu, užtikrinančiu susipažinimo įrodomumą, pirmojo prisijungimo prie Universiteto E. tapatybių valdymo sistemos ar Universiteto informacinio ištekliaus metu. Kai tokia galimybė Universiteto informaciniame ištekliuje nerealizuota, sutikimas turi būti patvirtinamas raštu, prieš naudotojui perduodant prieigos priemones.

8. Atnaujinus šias Taisykles, visi naudotojai su jomis susipažįsta ir patvirtina įsipareigojimus jų laikytis pakartotinai Taisyklių 6 punkte nurodytais būdais.

9. Naudotojai privalo saugoti duomenų ir informacijos paslaptį. Įsipareigojimas saugoti paslaptį galioja ir nutraukus su elektroninės informacijos tvarkymu susijusią veiklą.

10. Naudotojai ir naudotojų teisių administratoriai, pažeidę Taisyklių reikalavimus, atsako Universiteto vidaus tvarkos taisyklių ir kitų teisės aktų, kuriuose reglamentuojama atsakomybė už informacijos, kibernetinės ar elektroninių ryšių saugos bei susijusius pažeidimus, nustatyta tvarka.

II SKYRIUS
INFORMACINIŲ IŠTEKLIŲ NAUDOTOJŲ IR ADMINISTRATORIŲ ĮGALIOJIMAI, TEISĖS IR PAREIGOS

11. Padalinio, įgyvendinančio Universiteto informacinio ištekliaus valdymą, vadovas, kiek tai atitinka padalinio nuostatus, turi teisę:

11.1. pats tvarkyti savo padalinio valdomus informacinius išteklius ir leisti jais naudotis;

11.2. jei atsakomybės nenumatytos darbuotojo pareigybės aprašyme, skirti savo padalinio valdomų informacinių išteklių naudotojų teisių administratorius;

11.3. perduoti dalį savo padalinio valdomų informacinių išteklių tvarkymo funkcijų kitam padaliniui, su juo tai suderinus.

12. Kartą metuose ir ne vėliau kaip per 30 (trisdešimt) darbo dienų po struktūrinių pokyčių, padalinių, įgyvendinančių Universiteto informacinių išteklių valdymą, vadovai turi organizuoti naudotojams suteiktų prieigos teisių peržiūrą atrinktuose padaliniuose. Peržiūros rezultatai turi būti fiksuojami ir nustačius neatitikimą šioms Taisyklėms, suderinus su padalinio, įgyvendinančio Universiteto informacinio ištekliaus valdymą, vadovu, atliekamos prieigos teisių prie informacinio ištekliaus korekcijos.

13. Naudotojai privalo:

13.1. vesti tik tikslius duomenis;

13.2. užtikrinti tvarkomų duomenų konfidencialumą bei vientisumą;

13.3. pasikeitus paskyroje nurodytiems naudotojo asmens duomenims, informuoti padalinio, kuriam yra teikęs šiuos asmens duomenis, darbuotojus per 5 (penkias) darbo dienas nuo šių duomenų pasikeitimo arba per kitą su šiame papunktyje nurodytu darbuotoju sutartą terminą;

13.4. gavę nurodymą iš įgalioto asmens, nedelsiant, bet ne vėliau kaip per 5 (penkias) darbo dienas, ištaisyti pastebėtas klaidas ir informuoti apie atliktus veiksmus arba pateikti reikiamą informaciją apie planuojamus veiksmus, jei nurodymas negali būti įvykdytas nedelsiant;

13.5. savo veiksmais netrikdyti Universiteto informacinių išteklių darbo ir duomenų prieinamumo;

13.6. nesijungti prie centralizuotai valdomų Universiteto informacinių išteklių naudojantis kitiems naudotojams suteiktais prisijungimo vardais ir slaptažodžiais;

13.7. neatskleisti, nelaikyti matomoje vietoje suteiktų prisijungimo vardų ir slaptažodžių;

13.8. atsijungti nuo paskyros baigus darbą su Universiteto informaciniais ištekliais;

13.9. rinkti, tvarkyti, perduoti, įkelti, saugoti, naikinti ar kitaip informacinėse sistemose naudoti elektroninę informaciją tik naudojantis Universiteto suteikta darbo reikmėms paskyra;

13.10. baigus darbą užtikrinti, kad su elektronine informacija negalėtų susipažinti kiti asmenys, atsitraukiant nuo darbo vietos įjungti ekrano užsklandą su slaptažodžiu;

13.11. įgalioto asmens nurodymu naikinti elektroninę informaciją;

13.12. laikytis asmens duomenų apsaugą, kibernetinę ir informacijos saugą reglamentuojančių teisės aktų reikalavimų;

13.13. nedelsdami pranešti Universiteto Informacinių technologijų paslaugų centro Informacinių technologijų pagalbos skyriaus Naudotojų konsultavimo tarnybai (toliau – Naudotojų konsultavimo tarnyba) arba savo padalinio kompiuterizuotos darbo vietos administratoriui arba apie Universiteto informacinio ištekliaus veikimo sutrikimus, neįprastą jų veikimą, esamus arba galimus elektroninės informacijos saugumo reikalavimų pažeidimus, kitų naudotojų nederamus veiksmus.

14. Universiteto informacinių išteklių elektroninę informaciją tvarko naudotojų teisių administratoriai ir kiti administratoriai – sistemų administratoriai, programinės įrangos administratoriai, lokalaus tinklo ir kompiuterizuotų darbo vietų administratoriai.

15. Sistemų administratoriai:

15.1. tvarko administratorių teises;

15.2. įgaliotų asmenų nurodymu tvarko naudotojų teises ir paskyrų identifikavimo duomenis;

15.3. įgaliotų asmenų nurodymu tvarko naudotojų veiklos įrašus;

15.4. nustatyta vidaus tvarka ir terminais kuria atsargines elektroninės informacijos kopijas ir jas naikina.

16. Programinės įrangos administratoriai:

16.1. tvarko naudotojų veiklos įrašus;

16.2. įgaliotų asmenų nurodymu naikina elektroninę informaciją;

16.3. atlieka naudotojų teisių peržiūras;

16.4. įgaliotų asmenų nurodymu tvarko naudotojų teisių grupių aprašus (roles);

16.5. įgaliotų asmenų nurodymu rengia naudotojų teisių administravimo ataskaitas.

17. Naudotojų teisių administratoriai:

17.1. suteikia, keičia, stabdo, naikina ir kitaip tvarko naudotojų teises;

17.2. tvarko naudotojų paskyrų identifikavimo duomenis, jei netvarkoma automatiškai;

17.3. įgaliotų asmenų nurodymu naikina elektroninę informaciją;

17.4. įgaliotų asmenų nurodymu rengia naudotojų teisių administravimo ataskaitas;

17.5. atlieka naudotojų teisių peržiūras.

18. Lokalaus tinklo ir kompiuterizuotų darbo vietų administratoriai tvarko kompiuterizuotos darbo vietos sisteminės programinės įrangos, tinklo ir susijusios naudotojų veiklos įrašus.

19. Taisyklių 14 punkte nurodyti administratoriai turi teisę:

19.1. apie savo veiksmus iš anksto informuodami naudotoją, bet kada blokuoti naudotojo prieigą prie bet kurio Universiteto informacinio ištekliaus, jei naudotojas pažeidžia šių Taisyklių reikalavimus; informavimas iš anksto nėra būtinas, kai būtina operatyviai veikti blokuojant naudotojo prieigą dėl kilusios didelės grėsmės duomenų saugai.

19.2. reikalauti naudotojų patikslinti duomenis arba pateikti papildomos informacijos, jei to prireiktų Universiteto informacinių išteklių tvarkymo tikslams įgyvendinti.

20. Taisyklių 14 punkte nurodyti administratoriai, vykdydami savo tiesioginių vadovų, padalinių vadovų ir informacinių išteklių saugos įgaliotinių nurodymus, privalo suteikti informaciją įgaliotoms valstybės institucijoms apie naudotojus, kai ją būtina pateikti pagal Lietuvos Respublikos teisės aktų reikalavimus.

III SKYRIUS
SAUGAUS ELEKTRONINĖS INFORMACIJOS TEIKIMO INFORMACINIŲ IŠTEKLIŲ NAUDOTOJAMS KONTROLĖS TVARKA

21. Naudotojų prieigos registravimo ir stabdymo tvarka:

21.1. visi Universiteto bendruomenės nariai, siekiantys tapti Universiteto informacinių išteklių naudotojais, registruojasi Universiteto E. tapatybių valdymo sistemoje;

21.2. informacinių išteklių, neprijungtų prie Universiteto e-tapatybių sistemos, naudotojų prisijungimo duomenys naudotojams teikiami padalinių, įgyvendinančių Universiteto informacinių išteklių valdymą, nustatyta tvarka;

21.3. Universiteto bendruomenės narių, siekiančių tapti naudotojais, informacija, reikalinga naudotojo registracijai, automatiniu būdu gaunama iš Universiteto personalo valdymo informacinės sistemos ir Universiteto studijų informacinės sistemos;

21.4. naujas Universiteto bendruomenės narys, siekiantis tapti naudotoju, registracijos metu pateikia unikalų pirmojo prisijungimo kodą. Unikalų pirmojo prisijungimo kodą turi teisę gauti asmuo sudarantis darbo, studijų arba kitą sutartį ar pateikęs kitą dokumentą, kurio pagrindu asmuo tampa Universiteto bendruomenės nariu. Unikalų pirmojo prisijungimo kodą pateikia už šiame papunktyje nurodytų sutarčių ir (ar) kitų dokumentų sudarymą atsakingi asmenys;

21.5. kiti nei Taisyklių 21.1-21.4 papunktyje nurodyti asmenys, siekiantys tapti naudotojais (toliau – kiti naudotojai) ir gauti prieigą prie Universiteto informacinių išteklių, kuri jiems yra reikalinga siekiant užtikrinti kitų su Universitetu sudarytų sutarčių (pvz., paslaugų teikimo) įgyvendinimą arba kitais teisėtais pagrindais, gauna prisijungimo vardą ir laikiną slaptažodį, kurį turi pasikeisti pirmojo prisijungimo metu; šiame papunktyje nurodytiems asmenims prisijungimo vardą ir laikiną slaptažodį pateikia už paskyros sukūrimą atsakinga Naudotojų konsultavimo tarnyba arba padalinys, įgyvendinantis Universiteto informacinio ištekliaus valdymą;

21.6. prisijungimo duomenys pateikiami ne vėliau kaip per 2 (dvi) darbo dienas po sprendimo suteikti prieigos teises;

21.7. naudotojų teisių stabdymas (teisių apribojimas) įvyksta suėjus terminui, kuriam buvo teikta prieigos teisė, arba pasibaigus sutarčiai ar išnykus kitam teisėtam pagrindui, arba įgaliotų asmenų nurodymu, šiose Taisyklėse numatyta prieigos teisių peržiūros, keitimo ir naikinimo tvarka.

22. Naudotojų prieigos prie Universiteto informacinių išteklių teisių suteikimo tvarka:

22.1. suteikiant prieigą, nurodomas sutartyje, pareigybės aprašyme ar kitame dokumente, reglamentuojančiame naudotojo statusą, nurodytų funkcijų įgyvendinimui reikalingas minimalus Universiteto informacinių išteklių rinkinys;

22.2. suteikiant naudotojo prieigą prie papildomų Universiteto informacinių išteklių, reikalingas naudotojo teikiamas Taisyklių 24 punkte nustatyto turinio prašymas, parengtas Universiteto dokumentų valdymo sistemos priemonėmis, arba padalinio, įgyvendinančio informacinio ištekliaus valdymą, nustatytos formos prašymas;

22.3. prašymus teikia naudotojas, arba atsakingas sistemos valdymo arba tvarkymo funkcijas įgyvendinančio padalinio darbuotojas (toliau – kuratorius), jei naudotojas dėl objektyvių priežasčių negali pateiki prašymo pats;

22.4. prašymas turi būti suderintas su suinteresuoto padalinio vadovu ir padalinio, įgyvendinančio Universiteto informacinio ištekliaus valdymą ar tvarkymą, kai toks paskirtas vadovaujantis taisyklių 11.3 punktu, vadovu ar jo paskirtu darbuotoju;

22.5. prašymas turi būti pateikiamas ne vėliau kaip likus 2 (dviem) darbo dienoms iki pageidaujamų papildomų prieigos teisių suteikimo;

22.6. Informacinio ištekliaus valdymą įgyvendinantis padalinys ar Naudotojų konsultavimo tarnyba centralizuotai tvarkomų informacinių išteklių atveju, gavę prašymą, patikrina, ar prašymas suderintas su 22.4 papunktyje nurodytais asmenimis ir ar įtraukti visi numatyti duomenų valdytojai; jei reikalingi patikslinimai, prašymą grąžina rengėjui;

22.7. prašymas registruojamas ir ne vėliau kaip kitą darbo dieną perduodamas vykdyti prašyme nurodyto Universiteto informacinio ištekliaus naudotojų teisių arba sistemos administratoriui;

22.8. kai papildomas prieigos prie Universiteto informacinių išteklių teises prašoma suteikti laikinai, maksimalus laikino suteikimo terminas gali būti iki 1 (vienerių) metų;

22.9. suteikiant programinės įrangos licenciją, licencijos suteikimą Universiteto teisės aktų nustatyta tvarka registruoja kompiuterizuotos darbo vietos administratorius;

22.10. suteikus prašyme nurodytas prieigos teises arba atlikus veiksmus, kuriuos būtina atlikti siekiant gauti prieigą ar licenciją, apie tai informuojamas prašymą pateikęs naudotojas ir (ar) kuratorius. Prireikus, gali būti informuojami ir kiti asmenys.

23. Teisės administratoriams, duomenų valdymo ir saugos įgaliotiniams suteikiamos Taisyklių 22 punkte nustatyta tvarka, tačiau šiuo atveju prašymą teikią padalinio, kuriame dirba minėti asmenys, vadovas arba jo paskirtas padalinio darbuotojas, o sprendimą dėl teisių suteikimo priima padalinio, įgyvendinančio Universiteto informacinio ištekliaus valdymą, vadovas ar jo paskirtas padalinio darbuotojas.

24. Prieigos prie informacinių išteklių registravimo ir teisių suteikimo, keitimo ir šalinimo prašyme turi būti nurodoma ši informacija:

24.1. prieigos suteikimo teisinis pagrindas:

24.1.1. jei pagrindas yra sudaryta sutartis, nurodomas sutarties registracijos numeris ir data. Jei sutartį dar tik ketinama sudaryti, turi būti nurodyta data, kada ji bus sudaryta arba įsigalios;

24.1.2. jei prieigos teisės suteikiamos kitais teisėtais pagrindais, nurodomas kitas teisėtas pagrindas;

24.2. Universiteto informacinio ištekliaus pavadinimas, naudotojo padalinys arba padalinys, kuruojantis naudotoją, naudotojo vardas, pavardė, gimimo data (jei naudotojas nėra Universiteto bendruomenės narys), laikotarpis, kuriam reikalingos prieigos teisės (jeigu prieigos suteikimo teisinis pagrindas yra neterminuota sutartis, įrašoma „neterminuotai“);

24.3. prašomos suteikti Universiteto informacinio ištekliaus prieigos teisės (pvz., nurodomas rolės pavadinimas, teisių apimtis padaliniais, projektais, lėšų rūšimis).

25. Prieigos prie Universiteto informacinių išteklių peržiūros ir keitimo tvarka:

25.1. kai naudotojas perkeliamas į kitas pareigas Universitete arba pasikeičia naudotojo funkcijos, naudotojas, jo tiesioginis vadovas ar jo padalinio vadovo paskirtas padalinio darbuotojas Universiteto dokumentų valdymo sistemos priemonėmis parengia ir informacinio ištekliaus valdymą įgyvendinančiam padaliniui ar Naudotojų konsultavimo tarnybai pateikia Taisyklių 24 punkte nustatyto turinio prašymą dėl prieigos teisių peržiūros, kuriame nurodo naudotojo pareigų ir (ar) darbo funkcijų pasikeitimą ir (ar) prieigos prie konkrečių Universiteto informacinių išteklių poreikį;

25.2. naudotojų teisių administratorius naudotojų teisių peržiūrą pagal pateiktą prašymą atlieka ne vėliau kaip per 5 (penkias) dienas, išskyrus incidentų atvejus, kai teisės peržiūrimos nedelsiant, tą pačią arba sekančią darbo dieną.

26. Naudotojo ir (ar) administratoriaus prieiga prie Universiteto informacinių išteklių stabdymo ir (ar) naikinimo tvarka ir atvejai:

26.1. naudotojo ir (ar) administratoriaus prieigos prie Universiteto informacinių išteklių gali būti stabdoma ir (ar) naikinama:

26.1.1. nesutinkant ar atsisakius, kad būtų tvarkomi naudotojo paskyros asmens duomenys;

26.1.2. pasikeitus naudotojo užimamoms pareigoms ir funkcijoms;

26.1.3. naudotoją nušalinus nuo pareigų;

26.1.4. nustačius darbo pareigų ar kitokios sutarties pažeidimą;

26.1.5. įtarus galimą arba nustačius neteisėtą Universiteto informacinių išteklių arba naudotojo duomenų naudojimą;

26.1.6. gavus įgalioto asmens pranešimą apie konkretaus naudotojo prieigos prie konkrečių informacinių išteklių panaikinimą;

26.1.7. informacinių sistemų incidentų valdymo tvarkoje nustatytais atvejais;

26.1.8. kai administratorius nesijungė prie sistemos daugiau nei 3 (tris) mėnesius, o naudotojas nesijungė prie sistemos daugiau nei 6 (šešis) mėnesius;

26.1.9. vyksta administratoriaus ar naudotojo veiklos tyrimas;

26.1.10. administratoriui ar naudotojui atsisakius vykdyti įgaliotų asmenų nurodymus ir pavedimus.

26.2. naudotojo ir (ar) administratoriaus prieiga prie tvarkomų informacinių išteklių stabdoma ir (ar) naikinama teikiant Taisyklių 24 punkte nustatyto turinio prašymą arba nedelsiant įgalioto asmens nurodymu.

26.3. Naudotojų teisių administratorius naudotojų teisių stabdymą ir (ar) naikinimą pagal pateiktą prašymą atlieka ne vėliau kaip per 5 (penkias) dienas, išskyrus incidentų atvejus, kai teisės stabdomos nedelsiant, tą pačią arba sekančią darbo dieną.

26.4. Sustabdžius ir (ar) panaikinus prieigą, naudotojo paskyros registracijos duomenys elektroniniu būdu privalo būti saugomi ne trumpiau kaip 6 (šešis) mėnesius (išskyrus atvejus, numatytus kituose teisės aktuose), kuriems praėjus gali būti archyvuojami.

27. Prieigos prie Universiteto informacinių išteklių naikinimo tvarka:

27.1. naudotojams Universiteto bendruomenės nariams, pasibaigus jų sutartiniams santykiams su Universitetu arba teiktame prašyme nurodytam terminui, papildomai suteiktos prieigos teisės panaikinamos, tačiau 14 (keturiolikai) dienų paliekamas specialus Universiteto informacinių išteklių teisių ir prieigos rinkinys (pvz., elektroninis paštas), kuris suteikia prieigą tik prie paties naudotojo asmens duomenų. Suėjus šiame punkte nurodytam 14 (keturiolikos) dienų terminui prieiga naikinama automatiniu būdu;

27.2. kitiems naudotojams prieigos teisės naikinamos automatiniu būdu pasibaigus Taisyklių 22.2 punkte nurodyta tvarka teiktame prašyme nurodytam terminui arba anksčiau, pasibaigus sutartiniams santykiams su Universitetu arba išnykus arba pasibaigus kitam teisėtam pagrindui be pereinamojo laikotarpio;

27.3. naudotojo arba kuratoriaus argumentuotu prašymu, (pvz., siekiant pilno sutartinių įsipareigojimų įgyvendinimo, ar kitų darbo kodekse arba kolektyvinėje darbo sutartyje numatytų aplinkybių), informacinių išteklių valdytojo arba tvarkytojo funkcijas įgyvendinančio padalinio atsakingam asmeniui sutinkant, minimali prieiga gali būti pratęsta, bet ne ilgiau kaip 1 (vienerius) metus.

28. Priemonės naudotojų tapatybei nustatyti:

28.1. naudotojų tapatybei nustatyti prisijungiant prie Universiteto informacinio ištekliaus turi būti pateiktas prisijungimo prie Universiteto informacinių išteklių vardas, slaptažodis bei, kai įgyvendinta, pasinaudojama viena iš Taisyklių 28.4 papunktyje nurodytų kelių faktorių prisijungimo kontrolės sistemų;

Papunkčio pakeitimai:

Vilniaus universiteto rektoriaus 2024 m. lapkričio 8 d. įsakymu Nr. R-462

28.2. prisijungimo duomenys suteikiami tik Asmens duomenų tvarkymo Vilniaus universitete tvarkos apraše, patvirtintame Vilniaus universiteto rektoriaus 2018 m. gegužės 25 d. įsakymu Nr. R-316 „Dėl Asmens duomenų tvarkymo Vilniaus universitete tvarkos aprašo patvirtinimo“ (Vilniaus universiteto rektoriaus 2020 m. rugsėjo 25 d. įsakymo Nr. R-391 redakcija), numatyta tvarka patvirtintos tapatybės subjektams;

28.3. informacija, kaip prisijungti prie Universiteto informacinių išteklių, pateikiama supažindinimo su informaciniais ištekliais metu;

28.4. administratoriams ir naudotojams privaloma pasirinkti ir naudoti vieną iš kelių faktorių prisijungimo kontrolės sistemų:

28.4.1. programinius prieigos kodų generatorius (pvz., mobiliuosiuose telefonuose);

28.4.2. perskambinimą telefonu arba informavimą SMS žinute.

Papunkčio pakeitimai:

Vilniaus universiteto rektoriaus 2024 m. lapkričio 8 d. įsakymu Nr. R-462

28.5. kai leidžia techninės galimybės, administratoriams ir naudotojams, tvarkantiems asmens duomenis ar kitą konfidencialią informaciją, gali būti sudarytos galimybės naudoti kitas kelių faktorių prisijungimo kontrolės sistemas:

28.5.1. elektroninį parašą;

28.5.2. vardinį sertifikatą;

28.5.3. prieigos raktą;

28.5.4. biometrinę priemonę (pvz., piršto atspaudą).

Papunkčio pakeitimai:

Vilniaus universiteto rektoriaus 2024 m. lapkričio 8 d. įsakymu Nr. R-462

28.6. naudotojai, kurie prieigai prie Universiteto informacinių išteklių pageidauja naudoti 28.5 papunktyje įvardintas kelių faktorių prisijungimo sistemas, privalo pateikti prašymą Naudotojų konsultavimo tarnybai, kuri sprendimą dėl pateikto prašymo priima įvertinusi darbuotojo pareigybę ir atliekamas funkcijas.

Papildyta papunkčiu:

Vilniaus universiteto rektoriaus 2024 m. lapkričio 8 d. įsakymu Nr. R-462

29. Naudotojų slaptažodžių sudarymo, galiojimo trukmės ir keitimo reikalavimai:

29.1. pirmą kartą prisijungęs prie Universiteto E. tapatybių valdymo sistemos, naudotojas privalo pakeisti vienkartinį slaptažodį, jei toks buvo suteiktas;

29.2. naudotojui pamiršus slaptažodį, prieiga prie Universiteto informacinių išteklių suteikiama:

29.2.1. Universiteto E. tapatybių valdymo sistemos savitarnoje pateikus prieigos atstatymui būtinus duomenis, nurodomus Universiteto E. tapatybių valdymo sistemoje pirmo prisijungimo metu arba juos patikslinus kito prisijungimo metu;

29.2.2. naudotojo prašymu padalinio arba Naudotojų konsultavimo tarnybai.

29.3. naudotojas privalo saugoti slaptažodį ir jo neatskleisti tretiesiems asmenims, o įtaręs, kad tretieji asmenys sužinojo slaptažodį, privalo nedelsdamas jį pakeisti;

29.4. slaptažodis turi būti sudarytas iš ASCII koduotėje numatytų lotynų abėcėlės raidžių, skaičių ir specialiųjų simbolių;

29.5. slaptažodyje turi būti naudojama bent po vieną didžiąją ir mažąją raidę, skaičių ir specialų simbolį;

29.6. slaptažodyje negalima naudoti daugiau kaip du tuos pačius simbolius iš eilės;

29.7. slaptažodyje negali būti naudojami diakritiniai simboliai (taip pat lietuvių kalbos abėcėlės raidės ą, č, ę, ė, į, š, ų, ū, ž);

29.8. slaptažodyje nerekomenduojama naudoti šių specialių simbolių: /, :, !, \, %, |, $;

29.9. slaptažodžiams sudaryti neturi būti naudojama asmeninio pobūdžio informacija (pvz., gimimo data, šeimos narių vardai ir panašiai);

29.10. slaptažodžiams sudaryti neturi būti naudojami populiarūs vietovardžiai, asmenvardžiai ir kiti dažnai naudojami lietuvių ir anglų kalbų žodžiai;

29.11. jei kitaip nenustatyta atskirai tvirtinamuose Universiteto ar valstybės informacinių išteklių saugos politiką įgyvendinančiuose dokumentuose:

29.11.1. naudotojo paskyros slaptažodis turi būti keičiamas ne rečiau kaip kas 120 (šimtą dvidešimt) dienų;

29.11.2. naudotojo paskyros slaptažodis turi būti sudarytas iš ne mažiau kaip 8 (aštuonių) simbolių;

29.11.3. slaptažodžio galiojimo terminui artėjant į pabaigą, prieš 10 (dešimt) dienų ir 5 (penkias) dienas pakartotinai naudotojas turi būti įspėjamas pasikeisti slaptažodį;

29.11.4. Universiteto informaciniuose ištekliuose, kuriuose įgyvendintas kelių faktorių autentifikavimas, pagrindinis slaptažodis gali galioti vienerius metus, tačiau papildomo įrenginio kodas turi būti generuojamas unikaliai kiekvienai prisijungimo sesijai;

29.12. neadministruojantiems specialių kategorijų asmens duomenų ir kitos konfidencialios informacijos naudotojams, kai tai įgyvendinta informaciniame ištekliuje, leidžiama prisiminti autorizuotą įrenginį ir nereikalauti suvesti papildomo kodo. Ilgiau nei 30 (trisdešimt) dienų neprisijungus prie Universiteto informacinio ištekliaus, turi būti paprašoma papildomai autentifikuotis suvedant slaptažodį (ir papildomą kodą, kai naudotojas pasirinko naudoti kelių faktorių autentifikavimą);

29.13. keičiamas slaptažodis neturi sutapti su bent 6 (šešiais) prieš tai buvusiais slaptažodžiais;

29.14. neturi būti leidžiama pasikeisti slaptažodį antrą kartą per mažiau kaip 24 (dvidešimt keturias) valandas, išskyrus atvejį, kai žinoma, kad slaptažodis tapo žinomas kitam asmeniui. Tuo atveju Naudotojų konsultavimo tarnyba gali suteikti teisę pasikeisti slaptažodį dar kartą.

30. Papildomi konfidencialią informaciją arba kelių padalinių asmens duomenis tvarkančių naudotojų ir administratorių slaptažodžių tvarkymo reikalavimai:

30.1. slaptažodį turi sudaryti ne mažiau kaip 12 (dvylika) simbolių;

30.2. slaptažodis turi būti keičiamas ne rečiau kaip kas 3 (tris) mėnesius, išskyrus atvejus, kai prisijungimui naudojamos kelių faktorių autentifikavimo priemonės. Tokiu atveju pagrindinis slaptažodis gali galioti iki 180 (šimto aštuoniasdešimt) dienų.

30.3. Sistemoms, kuriose netvarkomi konfidencialūs ir (ar) asmens duomenys bei šių taisyklių 32 punkte nurodytiems specializuotiems technologiniams įrengimams galioja šių taisyklių 29.11 punkte nustatytas terminas.

31. Informacinių technologijų komponentai, patvirtinantys naudotojo tapatybę, turi drausti automatiškai išsaugoti slaptažodžius, išskyrus tinkamą saugos lygį užtikrinančias specializuotas slaptažodžių tvarkykles (pvz., slaptažodžių apsaugą dviem faktoriais įgyvendinančias programas).

32. Taisyklių 28-31 punktuose nurodyti reikalavimai specializuotiems technologiniams informaciniams ištekliams (specifinėms funkcijoms atlikti reikalinga informacinių išteklių infrastruktūra, techninė įranga, pvz. medicininė, matavimo ar eksperimentams atlikti reikalinga įranga, specializuota mokymo klasių ir laboratorinė įranga, meteorologinės ar metrologinės stotelės, specializuoti duomenų surinkimo įrenginiai, valdikliai ir SCADA įrenginiai, skaitikliai, duomenų šifravimo įrenginiai su gamintojo įdiegta šifravimo programine įranga ir pan. kuri yra gamintojo sukomplektuota su programine įranga, tačiau pagal savo paskirtį ir pobūdį negali būti talpinama duomenų centrų patalpose arba yra skirta specifinėms mokslinių tyrimų ar technologinių procesų funkcijomis atlikti) taikytini tiek, kiek juos leidžia įgyvendinti techninės galimybės, tačiau negali būti nustatyti silpnesni reikalavimai, nei numatyta Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašo 1 priede.

33. Universiteto informaciniuose ištekliuose (kai tai leidžia techninės galimybės) turi būti įgyvendintos šios prieigos prie paskyros atstatymo priemonės:

33.1. patvirtinimo kodo atsiuntimas į naudotojo paskyroje nurodytą ir patvirtintą ES operatoriaus mobiliojo telefono numerį;

33.2. nuorodos į prieigos atstatymo formą atsiuntimas į naudotojo paskyroje nurodytą atsarginį asmeninį el. pašto adresą;

33.3. Universiteto E. tapatybių valdymo sistemos savitarnos puslapyje panaudojant paskyros kūrimo metu įvedamą tik naudotojui žinomą ne trumpesnę nei 12 simbolių aplinkybę ar raktinę frazę;

33.4. skambutis Naudotojų konsultavimo tarnybos darbuotojams tel. (8 5) 236 6200 iš naudotojo paskyroje nurodyto atsarginio paskyros atstatymo telefono, patvirtinant paskyros kūrimo metu nurodytą slaptą frazę ir du asmens duomenis (asmens kodą, darbuotojo tabelinį ar studento pažymėjimo numerį, kontaktinio asmens nelaimės atveju vardą ir pavardę). Siekdami užtikrinti, kad tokiu būdu negalėtų būti užvaldoma paskyra, Naudotojų konsultavimo tarnybos darbuotojai turi teisę užduoti ir kitus šiame papunktyje nenumatytus papildomus asmens tapatybės nustatymo klausimus;

33.5. pakeitus slaptažodį, naudotojas turi gauti tekstinį pranešimą apie bandymą prisijungti naudotojo paskyroje nurodytu elektroniniu paštu ir mobiliojo telefono numeriu.

34. Turi būti nustatytas didžiausias leistinas naudotojo mėginimų įvesti teisingą slaptažodį, frazę arba pažymėti teisingą vaizdą (reCAPTHA) skaičius (ne daugiau kaip 5 (penki) kartai per 15 (penkiolika) minučių iš to paties IP adreso, jei informacinis išteklius palaiko tokį funkcionalumą). Iš eilės neteisingai įvedus slaptažodį ar pažymėjus vaizdą tiek kartų, kiek nustatyta, naudotojo paskyros prieiga iš šio IP adreso turi užsirakinti ir neleisti naudotojui jungtis ne trumpiau kaip 15 (penkiolika) minučių. Kai tai leidžia techninės galimybės, pasirinktu paskyros atstatymo (atsarginiu) kontaktu naudotojas turi gauti tekstinį pranešimą apie bandymą prisijungti naudotojo paskyroje nurodytais pagrindiniais elektroninio pašto ir mobilaus telefono numeriais.

35. Administratoriai ir naudotojai, tvarkantys kitų asmenų duomenis ar kitą konfidencialią informaciją nuotoliniu būdu, privalo prisijungimui prie informacinių išteklių naudoti Vilniaus universiteto virtualų privatų tinklą arba kitokį saugų tunelį, t. y. prisijungimas prie informacinių išteklių galimas tik naudojantis šifruotu kanalu. Ryšys turi būti šifruojamas naudojant ne trumpesnį kaip 256 bitų raktą.

36. Prisijungimai ir (ar) bandymai prisijungti prie Universiteto informacinių išteklių IP tinklais automatiškai registruojami veiksmų žurnaluose. Registracijos duomenys apima prisijungimo ir (ar) bandymo prisijungti datą, laiką, prisijungimo trukmę (jei buvo prisijungta), prisijungusio ar bandžiusio prisijungti naudotojo vardą ir kompiuterio, iš kurio buvo prisijungta ar bandyta prisijungti IP adresą, funkcijas, prie kurių buvo jungtasi, atliktų veiksmų su asmens duomenimis (įvedimas, peržiūra, keitimas, naikinimas ir kiti duomenų tvarkymo veiksmai) sąrašą. Šie įrašai saugomi ne trumpiau kaip 6 (šešis) mėnesius.

_____