informatikos ir ryšių departamentas

VALSTYBĖS INFORMACINIŲ SISTEMŲ IR REGISTRŲ ELEKTRONINĖS INFORMACIJOS SAUGOS UŽTIKRINIMAS

Vilnius
2017-12-14

Elektroninės informacijos saugos teisinis reglamentavimas. Pagrindiniai teisės aktai

Įstatymai

- Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymas
- Lietuvos Respublikos kibernetinio saugumo įstatymas

Vyriausybės nutarimai

- 2013-07-24 nutarimas Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo patvirtinimo“ (keistas LRV 2016-08-11 nutarimu Nr. 826)
- 2016 m. balandžio 20 d. nutarimas Nr. 387 „Dėl Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų ypatingos svarbos informacinei infrastruktūrai ir valstybės informaciniams ištekliams, aprašo patvirtinimo“

VALSTYBĖS INFORMACINIŲ IŠTEKLIŲ SAUGA VIIS
Valstybės informacinių išteklių valdymo įstatymas
Vyriausybės 2013 m. liepos 24 d. nutarimas Nr. 716 „Dėl **Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo** patvirtinimo“, pakeistas 2016 08 11 nutarimu Nr. 826 (TAR, 2016, Nr. 2016-22452)
Vyriausybės 2011 m. birželio 29 d. nutarimas Nr. 796 „Dėl Elektroninės informacijos saugos (kibernetinio saugumo) plėtros 2011-2019 metais programos patvirtinimo“ (Žin., 2011, Nr. 83-4033)
Vidaus reikalų ministro 2013 m. spalio 4 d. įsakymas Nr. 1V-832 „Dėl **Techninių valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimų** patvirtinimo“ (Žin., 2013, Nr. 106-5251)
Vidaus reikalų ministro 2012 m. spalio 16 d. įsakymas Nr. 1V-740 „Dėl Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemos nuostatų patvirtinimo“ (Žin., 2012, Nr. 123-6204)
Vidaus reikalų ministro 2004 m. gegužės 6 d. įsakymas Nr. 1V-156 „Dėl Informacinių technologijų **saugos atitikties vertinimo metodikos** patvirtinimo“ (Žin., 2004, Nr. 80-2855; TAR, 2016-08-02, Nr. 2016-21233)
Valstybinės duomenų apsaugos inspekcijos direktoriaus 2008 m. lapkričio 12 d. įsakymas Nr. 1T-71(1.12) „Dėl Bendrųjų reikalavimų organizacinėms ir techninėms duomenų saugumo priemonėms patvirtinimo (Dėl Bendrųjų reikalavimų organizacinėms ir techninėms **asmens duomenų saugumo** priemonėms patvirtinimo)“ (Žin., 2008, Nr. 135-5298)
Vidaus reikalų ministerijos parengtas **Rizikos vertinimo vadovas**.
Standartai: LST EN ISO/IEC 27001:2017 ir Informacinės technologijos. Saugumo metodai. Informacijos saugumo valdymo sistemos. Reikalavimai. LST EN ISO/IEC 27002:2017 Informacinės technologijos. Saugumo metodai. Informacijos saugumo kontrolės priemonių praktikos nuostatai.

Kibernetinio saugumo įstatymas
Vyriausybės 2016 m. balandžio 20 d. nutarimas Nr. 387 „Dėl **Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų ypatingos svarbos informacinei infrastruktūrai ir valstybės informaciniams ištekliams, aprašo** patvirtinimo“ (TAR, 2016-04-26, Nr. 2016-10368),
Vyriausybės 2016 m. sausio 25 d. nutarimas Nr. 87 „Dėl Nacionalinio kibernetinių incidentų valdymo plano patvirtinimo“ (TAR, 2016-01-28, Nr. 2016-01717)
Vyriausybės 2016 m. liepos 20 d. nutarimas Nr. 746 „Dėl Tipinio kibernetinių incidentų valdymo ypatingos svarbos informacinėse infrastruktūrose plano patvirtinimo“ (TAR, 2016-07-22, Nr. 2016-20914)
Vyriausybės 2016 m. liepos 20 d. nutarimas Nr. 742 „Dėl Ypatingos svarbos informacinės infrastruktūros identifikavimo metodikos patvirtinimo“ (TAR, 2016-07-21, Nr. 2016-20862) http://vrm.lrv.lt/lt/veiklos-sritys/elektronines-informacijos-sauga-1
Krašto apsaugos ministro 2015 m. gegužės 5 d. įsakymas Nr. V-461 „Dėl Techninių kibernetinio saugumo priemonių diegimo ir valdymo valstybės informaciniuose ištekliuose ir ypatingos svarbos informacinėje infrastruktūroje tvarkos aprašo patvirtinimo“ (TAR, 2015-05-06, Nr. 2015-06797)
Krašto apsaugos ministro 2016 m. sausio 6 d. įsakymas Nr. V-11 „Dėl Nacionalinio kibernetinio saugumo centro reagavimo į kibernetinius incidentus valstybės informaciniuose ištekliuose ir ypatingos svarbos informacinėse infrastruktūrose tvarkos aprašo patvirtinimo“ (TAR, 2016-01-07, Nr. 2016-00407)
Lietuvos policijos generalinio komisaro 2015 m. vasario 2 d. įsakymas Nr. 5-V-101 „Dėl Informacijos, reikalingos kibernetiniams incidentams, galimai turintiems nusikalstamos veikos požymių, užkardyti ir tirti, pateikimo, policijos nurodymų vykdymo bei kibernetinių incidentų tyrimo tvarkos aprašo patvirtinimo“ (TAR, 2015-02-03, Nr. 2015-01654)
Valstybinės duomenų apsaugos inspekcijos direktoriaus 2015 m. vasario 25 d. įsakymas Nr. 1T-11(1.12.E) „Dėl Informacijos apie kibernetinius incidentus, susijusius su asmens duomenų saugumo pažeidimais, ir taikytas šių incidentų valdymo priemones pateikimo Valstybinei duomenų apsaugos inspekcijai tvarkos aprašo ir rekomenduojamos Informacijos apie kibernetinius incidentus, susijusius su asmens duomenų saugumo pažeidimais, ir taikytas šių incidentų valdymo priemones pateikimo Valstybinei duomenų apsaugos inspekcijai formos patvirtinimo“ (TAR, 2015-02-25, Nr. 2015-02942)

Teisės aktai. Sistemų ir registrų steigimas ir įteisinimas

- LRV 2013-02-27 nutarimas Nr. 180 „Dėl Valstybės informacinių sistemų steigimo, kūrimo, modernizavimo ir likvidavimo tvarkos aprašo patvirtinimo“
- IVPK prie SM 2014 m. vasario 25 d. įsakymas Nr. T-29 „Dėl Valstybės informacinių sistemų gyvavimo ciklo valdymo metodikos patvirtinimo“
- VRM 2013-09-27 įsakymas Nr. 1V-807 „Dėl Informacinių sistemų, kuriomis tvarkoma informacija, susijusi su **personalo** valdymu, steigimo, kūrimo, modernizavimo ir likvidavimo tvarkos aprašo patvirtinimo“
- Lietuvos vyriausiojo archyvaro 2013-06-18 įsakymas Nr. V-45 „Dėl Informacinių sistemų, kuriomis tvarkoma informacija, susijusi su **dokumentų** valdymu, steigimo, kūrimo, modernizavimo ir likvidavimo tvarkos aprašo patvirtinimo“
- FM 2013-10-07 įsakymas Nr. 1K-334 „Dėl Informacinių sistemų, kuriomis tvarkoma informacija, susijusi su **materialinių ir finansinių išteklių** valdymu, steigimo, kūrimo, modernizavimo ir likvidavimo tvarkos aprašo patvirtinimo“

Standartai

Saugos srities standartai:

- LST EN ISO/IEC 27001:2017 Informacinės technologijos. Saugumo metodai. Informacijos saugumo valdymo sistemos. Reikalavimai.
- LST EN ISO/IEC 27002:2017 Informacinės technologijos. Saugumo metodai. Informacijos saugumo kontrolės priemonių praktikos nuostatai.

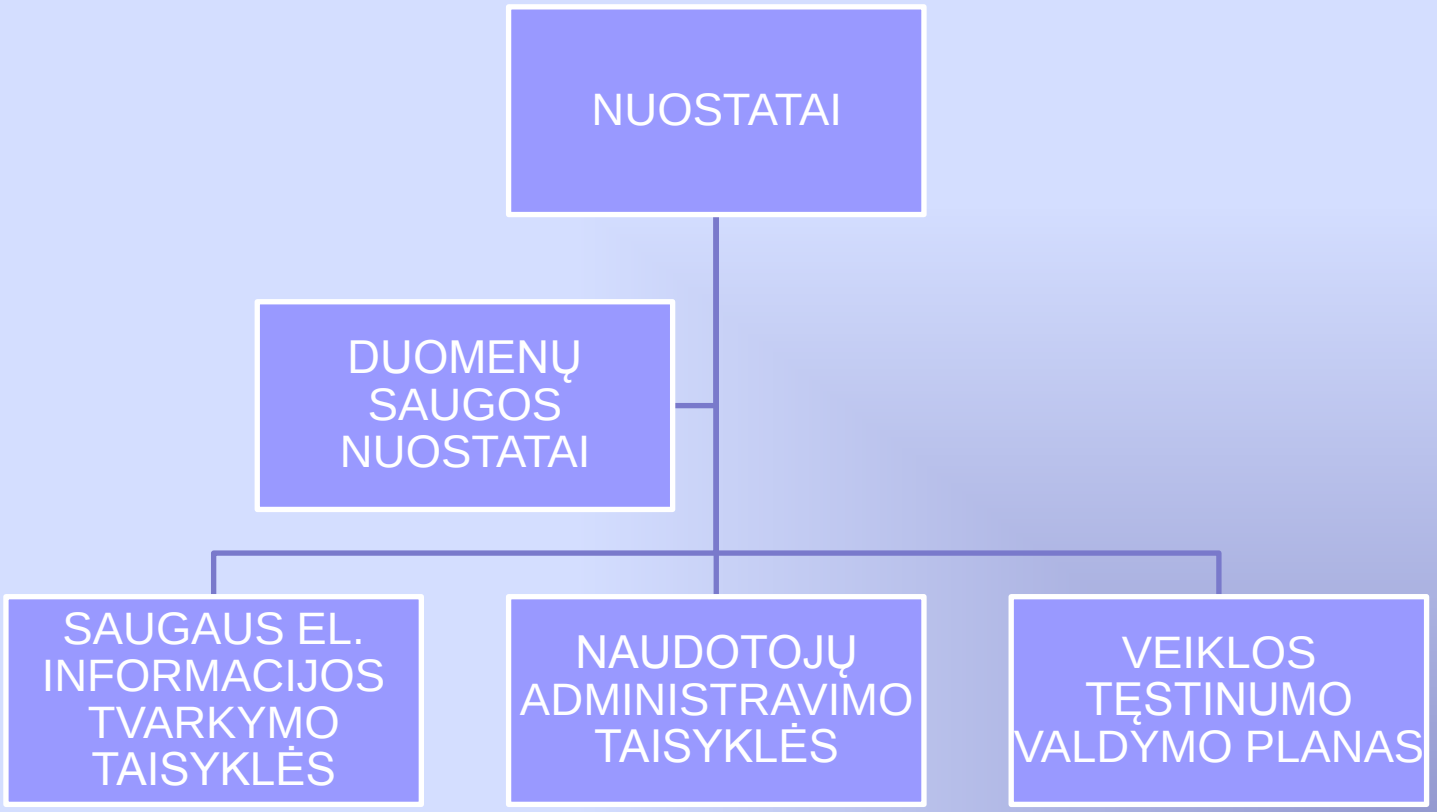
Vidaus reikalų srities informacinių sistemų ir registrų saugos politika

- **Bendri duomenų saugos nuostatai** Vidaus reikalų ministerijos valdomų bei Informatikos ir ryšių departamento tvarkomų informacinių sistemų ir registrų. *Projektas „Dėl kai kurių Lietuvos Respublikos vidaus reikalų ministerijos valdomų registrų ir valstybės informacinių sistemų duomenų saugos nuostatų patvirtinimo“*
- **Techninių kibernetinio saugumo reikalavimų įgyvendinimo** Vidaus reikalų ministerijos valdomuose ypatingos svarbos informacinėse infrastruktūrose ir valstybės informaciniuose ištekliuose priemonių planas, patvirtintas 2017 m. rugsėjo 20 d. Nr. 1V-650
- **Kibernetinių incidentų valdymo** Vidaus reikalų ministerijos valdomose ypatingos svarbos informacinėse infrastruktūrose planas, patvirtintas 2017 m. rugsėjo 20 d. Nr. 1V-651
- Vidaus reikalų ministerijos valdomų registrų ir informacinių sistemų pokyčių valdymo tvarkos aprašas
- Vidaus reikalų ministerijos darbo reglamentas (Informacinių technologijų ir telekomunikacinės įrangos naudojimas tarnybinių komandiruočių metu)

PAGRINDINIAI TEISINIO REGLAMENTAVIMO POKYČIAI IR NAUJOVĖS

- ✓ Pakeistas Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašas (LRV 2016 08 11 nutarimu Nr. 826 (TAR, 2016, Nr. 2016-22452)
- ✓ Naujas Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų ypatingos svarbos informacinei infrastruktūrai ir valstybės informaciniams ištekliams, aprašas (TAR, 2016-04-26, Nr. 2016-10368)
- ✓ Nauja Ypatingos svarbos informacinės infrastruktūros identifikavimo metodika (TAR, 2016-07-21, Nr. 2016-20862)
- ✓ Pakeista Informacinių technologijų saugos atitikties vertinimo metodika (TAR, 2016-08-02, Nr. 2016-21233)

SAUGOS POLITIKOS REGLAMENTAVIMAS: PAGRINDINIAI DOKUMENTAI



Kibernetinio saugumo nuostatų reglamentavimo alternatyvos

I	II
Papildyti turimus saugos dokumentus kibernetinio saugumo nuostatomis	Parengti naują kibernetinio saugumo politikos dokumentą

IS/R KLASIFIKAVIMO POKYČIAI NUO 2016-08-19, PRIĖMUS VYRIAUSYBĖS 2016-08-11 NUTARIMĄ NR. 826

Naujoji redakcija	Senoji redakcija	Komentaras
1. ypatingos svarbos informacija; 2. svarbi informacija; 3. vidutinės svarbos informacija; 4. mažiausios svarbos informacija.	ypatingos svarbos el. informacija, svarbi el. informacija, žinybinės svarbos el. informacija kita elektroninė informacija	vietoj „žinybinės svarbos“ – „vidutinės svarbos, vietoj „kita informacija“ – „mažiausios svarbos informacija“.

12. Informacinės sistemos pagal jose tvarkomos informacijos svarbą skirstomos į 4 kategorijas (pirmoji – aukščiausioji, ketvirtoji – žemiausioji kategorija):	**5. Valstybės registrai (kadastrai), žinybiniai registrai, valstybės informacinės sistemos ir kitos informacinės sistemos klasifikuojamos pagal kategorijas nuo pirmos (aukščiausioji kategorija) iki ketvirtos (žemiausioji kategorija) pagal jose apdorojamos informacijos svarbos kategoriją:**	
12.1. pirmajai kategorijai priskiriamos informacinės sistemos, kuriose tvarkoma ypatingos svarbos informacija;	5.1. Pirmai kategorijai priskiriami pagrindiniai valstybės registrai, kiti valstybės registrai (kadastrai) ir valstybės informacinės sistemos, kuriuose apdorojama ypatingos svarbos elektroninė informacija.	1 kategorijai automatiškai nebepriskiriami pagrindiniai valstybės registrai (kadastrai), jie vertinami pagal bendrus kriterijus ir gali būti priskirti bet kuriai kategorijai.
12.2. antrajai kategorijai priskiriamos informacinės sistemos, kuriose tvarkoma svarbi informacija;	5.2. Antrai kategorijai priskiriami valstybės registrai (kadastrai), valstybės informacinės sistemos, kuriuose apdorojama svarbi elektroninė informacija.	2 kategorijai automatiškai nebepriskiriami valstybės registrai (kadastrai), jie vertinami pagal bendrus kriterijus ir gali būti priskirti bet kuriai kategorijai.
12.3. trečiajai kategorijai priskiriamos informacinės sistemos, kuriose tvarkoma vidutinės svarbos informacija;	5.3. Trečiai kategorijai priskiriami žinybiniai registrai, valstybės informacinės sistemos, kuriuose apdorojama žinybinės svarbos elektroninė informacija.	3 kategorijai automatiškai nebepriskiriami žinybiniai registrai (kadastrai), jie vertinami pagal bendrus kriterijus ir gali būti priskirti bet kuriai kategorijai.
12.4. ketvirtajai kategorijai priskiriamos informacinės sistemos, kuriose tvarkoma mažiausios svarbos informacija.	5.4. Ketvirtai kategorijai priskiriamos kitos informacinės sistemos, kuriose apdorojama vidaus administravimo informacija.	Iki šiol pagal VIIVĮ kitais informaciniais ištekliais buvo laikomos vidaus administravimo IS ir jos automatiškai buvo priskiriamos 4 kat., dabar jos vertinamos pagal bendrus kriterijus ir gali būti priskirtos bet kuriai kategorijai.

REIKALAVIMAI INFORMACINIŲ SISTEMŲ IR REGISTRŲ NAUDOTOJAMS (apibendrinti) I

- ✓ Tvarkyti informacinės sistemos ir registro elektroninę informaciją gali tik registro ir informacinės sistemos naudotojai (toliau – naudotojai), susipažinę su registro ir informacinės sistemos saugos dokumentais ir sutikę laikytis jų reikalavimų.
- ✓ Naudotojai, tvarkantys duomenis, informaciją, dokumentus ir (arba) jų kopijas, privalo įsipareigoti saugoti duomenų ir informacijos paslaptį. Įsipareigojimas saugoti paslaptį galioja ir nutraukus su duomenų, informacijos, dokumentų ir (arba) jų kopijų tvarkymu susijusią veiklą bei valstybės tarnybos ar darbo santykius.
- ✓ Naudotojai, atliekantys tarnybines funkcijas, susijusias su asmens duomenų tvarkymu bei teikimu, raštu pasirašytinai įpareigojami saugoti asmens duomenų paslaptį. Asmens duomenų paslaptį jie privalo saugoti ir pasibaigus darbo (tarnybos) santykiams, per visą asmens duomenų teisinės apsaugos laiką, jeigu įstatymas nenumato ko kita.
- ✓ Naudotojas turi patvirtinti savo tapatybę slaptažodžiu, taip pat kita tapatumo patvirtinimo priemone, kurios reikalaujama jungiantis prie konkrečios informacinės sistemos ar registro.
- ✓ Naudotojas, pamiršęs, praradęs arba kitaip netekęs savo prisijungimo prie informacinės sistemos ir registro vardo ir (ar) slaptažodžio, turi nedelsdamas elektroniniu paštu arba telefonu informuoti informacinių technologijų pagalbos tarnybą (toliau – ITT pagalbos tarnyba) arba IS administratorių.

REIKALAVIMAI INFORMACINIŲ SISTEMŲ IR REGISTRŲ NAUDOTOJAMS (apibendrinti) II

- ✓ Slaptažodis turi būti sudarytas iš raidžių, skaičių ir specialiųjų simbolių.
- ✓ Slaptažodis turi būti ne trumpesnis nei aštuonių simbolių.
- ✓ Slaptažodžiams sudaryti neturi būti naudojama asmeninio pobūdžio informacija (pavyzdžiui, gimimo data, šeimos narių vardai ir panašiai).
- ✓ Draudžiama slaptažodžius atskleisti kitiems asmenims ar pastariesiems sudaryti galimybę juos sužinoti (pvz., užrašyti slaptažodį ant lapelio ir palikti darbo vietoje).
- ✓ Naudotojo teisė dirbti su konkrečia informacine sistema ar registru turi būti sustabdoma, kai naudotojas nesinaudoja informacine sistema ar registru ilgiau kaip 3 mėnesius (jeigu IS dalys palaiko tokį funkcionalumą).
- ✓ Kai įstatymų nustatytais atvejais naudotojas nušalinamas nuo darbo (pareigų), neatitinka kituose teisės aktuose nustatytų naudotojo kvalifikacinių reikalavimų, praranda patikimumą, taip pat kai pasibaigia jo darbo (tarnybos) santykiai, jo teisė naudotis informacine sistema ar registru turi būti panaikinta nedelsiant.
- ✓ Naudotojui neatliekant su informacine sistema ar registru jokių veiksmų, darbo stotis turi užsirakinti, kad toliau naudotis ja būtų galima tik pakartotinai patvirtinus savo tapatybę. Laikas, per kurį naudotojui neatliekant jokių veiksmų darbo stotis turi užsirakinti, negali būti ilgesnis kaip 15 minučių.
- ✓ Baigus darbą ar naudotojui pasitraukiant iš darbo vietos, turi būti imamasi priemonių, kad su informacija, kuri tvarkoma informacinėje sistemoje ar registre, negalėtų susipažinti kiti asmenys: atsijungiama nuo informacinės sistemos ar registro, įjungiama ekrano užsklanda su slaptažodžiu.
- ✓ Naudotojai, pastebėję saugos dokumentuose nustatytų reikalavimų pažeidimų, nusikalstamos veikos požymių, neveikiančias arba netinkamai veikiančias saugos užtikrinimo priemones, privalo nedelsdami pranešti apie tai ITT pagalbos tarnybai arba IS administratoriui ar saugos įgaliotiniui.

REIKALAVIMAI INFORMACINIŲ SISTEMŲ IR REGISTRŲ NAUDOTOJAMS (apibendrinti) III

Naudotojams draudžiama:

- ✓ atskleisti informacinės sistemos duomenis ar suteikti kitokią galimybę bet kokia forma su jais susipažinti tokios teisės neturintiems asmenims;
- ✓ savavališkai diegti informacinės sistemos taikomosios programinės įrangos pakeitimus ir naujas versijas neturint tam suteiktos teisės;
- ✓ atskleisti kitiems asmenims prisijungimo prie informacinės sistemos vardą, slaptažodį ar kitaip sudaryti sąlygas jais pasinaudoti;
- ✓ naudoti informacinės sistemos duomenis kitokiais nei jų nuostatuose nurodytais tikslais bei savo pareigybės aprašyme nustatytų funkcijų vykdymo tikslais;
- ✓ sudaryti sąlygas pasinaudoti informacinei sistemai tvarkyti naudojama technine ir programine įranga tokios teisės neturintiems asmenims (paliekant darbo vietą būtina užrakinti darbalaukį arba išjungti darbo stotį);
- ✓ atlikti veiksmus, dėl kurių gali būti neteisėtai pakeisti, sunaikinti ar atskleisti informacinės sistemos duomenys, taip pat neatlikti būtinų veiksmų, kurie apsaugo informacinės sistemos duomenis;
- ✓ atlikti bet kokius kitus neteisėtus informacinės sistemos tvarkymo veiksmus.

informatikos ir ryšių departamentas

Sauga – ne produktas, o procesas

Renata Mačiulevičienė
2017 m. gruodžio 14 d.