LIETUVOS RESPUBLIKOS VIDAUS REIKALŲ MINISTRO

Į S A K Y M A S
DĖL VALSTYBĖS INSTITUCIJŲ IR ĮSTAIGŲ INFORMACINIŲ SISTEMŲ ELEKTRONINĖS INFORMACIJOS TECHNINIŲ SAUGOS REIKALAVIMŲ PATVIRTINIMO IR LIETUVOS RESPUBLIKOS VIDAUS REIKALŲ MINISTRO 2007 M. LIEPOS 11 D. ĮSAKYMO NR. 1V-247 „DĖL VALSTYBĖS INSTITUCIJŲ IR ĮSTAIGŲ INFORMACINIŲ SISTEMŲ KLASIFIKAVIMO PAGAL JOSE TVARKOMĄ ELEKTRONINĘ INFORMACIJĄ GAIRIŲ IR VALSTYBĖS INSTITUCIJŲ IR ĮSTAIGŲ INFORMACINIŲ SISTEMŲ ELEKTRONINĖS INFORMACIJOS SAUGOS REIKALAVIMŲ PATVIRTINIMO“ PAKEITIMO

2008 m. spalio 27 d. Nr. 1V-384
Vilnius

Vadovaudamasis Bendrųjų elektroninės informacijos saugos valstybės institucijų ir įstaigų informacinėse sistemose reikalavimų, patvirtintų Lietuvos Respublikos Vyriausybės 1997 m. rugsėjo 4 d. nutarimu Nr. 952 (Žin., 1997, Nr. 83-2075; 2007, Nr. 49-1891; 2008, Nr. 85-3393), 2 punktu:

1. T v i r t i n u Valstybės institucijų ir įstaigų informacinių sistemų elektroninės informacijos techninius saugos reikalavimus (pridedama).

2. P a k e i č i u Lietuvos Respublikos vidaus reikalų ministro 2007 m. liepos 11 d. įsakymą Nr. 1V-247 „Dėl Valstybės institucijų ir įstaigų informacinių sistemų klasifikavimo pagal jose tvarkomą elektroninę informaciją gairių ir Valstybės institucijų ir įstaigų informacinių sistemų elektroninės informacijos saugos reikalavimų patvirtinimo“ (Žin., 2007, Nr. 78-3160):

2.1. Išdėstau antraštę taip:

„DĖL VALSTYBĖS INSTITUCIJŲ IR ĮSTAIGŲ INFORMACINIŲ SISTEMŲ KLASIFIKAVIMO PAGAL JOSE TVARKOMĄ ELEKTRONINĘ INFORMACIJĄ GAIRIŲ PATVIRTINIMO“.

2.2. Pripažįstu netekusiu galios 1.2 punktą.

VIDAUS REIKALŲ MINISTRAS REGIMANTAS ČIUPAILA

PATVIRTINTA
Lietuvos Respublikos vidaus reikalų
ministro 2008 m. spalio 27 d.
įsakymu Nr. 1V-384

VALSTYBĖS INSTITUCIJŲ IR ĮSTAIGŲ INFORMACINIŲ SISTEMŲ ELEKTRONINĖS INFORMACIJOS TECHNINIAI SAUGOS REIKALAVIMAI

I. BENDROSIOS NUOSTATOS

1. Valstybės institucijų ir įstaigų informacinių sistemų elektroninės informacijos techninių saugos reikalavimų (toliau – reikalavimai) tikslas – nustatyti minimalius elektroninės informacijos techninius saugos reikalavimus Lietuvos Respublikos Vyriausybei atskaitingų valstybės institucijų ir įstaigų (toliau – institucija) informacinėms sistemoms (toliau – informacinės sistemos).

2. Reikalavimuose vartojamos sąvokos:

Konfidencialumas – elektroninės informacijos savybė – su informacinėje sistemoje tvarkoma elektronine informacija gali susipažinti tik tam įgalioti asmenys.

Vientisumas – elektroninės informacijos savybė – elektroninė informacija nebuvo atsitiktiniu ar neteisėtu būdu pakeista ar sunaikinta.

Prieinamumas – elektroninės informacijos savybė – elektroninė informacija gali būti tvarkoma reikiamu metu.

Sauga – elektroninės informacijos konfidencialumo, vientisumo ir prieinamumo užtikrinimas.

Kitos reikalavimuose vartojamos sąvokos atitinka sąvokas, nustatytas Bendruosiuose elektroninės informacijos saugos valstybės institucijų ir įstaigų informacinėse sistemose reikalavimuose, patvirtintuose Lietuvos Respublikos Vyriausybės 1997 m. rugsėjo 4 d. nutarimu Nr. 952 (Žin., 1997, Nr. 83-2075; 2007, Nr. 49-1891), Lietuvos Respublikos įstatymuose ir kituose teisės aktuose.

II. INFORMACINIŲ SISTEMŲ ELEKTRONINĖS INFORMACIJOS TECHNINIAI SAUGOS REIKALAVIMAI

3. Bendrieji informacinių sistemų elektroninės informacijos techniniai saugos reikalavimai:

3.1. turi būti periodiškai atliekamas informacinės sistemos informacinių technologijų saugos atitikties vertinimas (toliau – atitikties vertinimas);

3.2. informacinė sistema turi registruoti bent vieną paskutinį informacinės sistemos elektroninės informacijos pakeitimą atlikusį informacinės sistemos naudotoją ir pakeitimo laiką;

3.3. informacinės sistemos priežiūros funkcijos turi būti atliekamos naudojant atskirą tam skirtą administratoriaus identifikatorių, kuriuo naudojantis nebūtų galima atlikti informacinės sistemos naudotojo funkcijų;

3.4. kiekvienas informacinės sistemos naudotojas turi būti informacinėje sistemoje unikaliai identifikuojamas – informacinės sistemos naudotojas turi patvirtinti savo tapatybę slaptažodžiu arba kita autentiškumo patvirtinimo priemone;

3.5. informacinės sistemos naudotojui teisė dirbti su konkrečia elektronine informacija turi būti ribojama ar sustabdoma, kai informacinės sistemos naudotojas atostogauja, vykdomas informacinės sistemos naudotojo veiklos tyrimas ir pan.; pasibaigus tarnybos (darbo) santykiams, informacinės sistemos naudotojo teisė naudotis informacine sistema turi būti panaikinta;

3.6. baigus darbą turi būti imamasi priemonių, kad su elektronine informacija negalėtų susipažinti pašaliniai asmenys: atsijungiama nuo informacinės sistemos, įjungiama ekrano užsklanda su slaptažodžiu, dokumentai padedami į pašaliniams asmenims neprieinamą vietą ir pan.;

3.7. informacinės sistemos naudotojui neatliekant jokių veiksmų, informacinė sistema turi užsirakinti, kad toliau naudotis informacine sistema galima būtų tik pakartojus tapatybės nustatymo ir autentiškumo patvirtinimo veiksmus;

3.8. institucija turi išsiaiškinti, kiek ji ilgiausiai gali tęsti savo funkcijų įgyvendinimą neveikiant informacinei sistemai ar jos daliai; institucijos informacinės sistemos veiklos tęstinumo valdymo planas turi užtikrinti informacinės sistemos veiklos atkūrimą per šį laikotarpį; turi būti parengtas veiksmų planas, užtikrinantis informacinės sistemos veiklos atnaujinimą ketvirtosios kategorijos informacinėms sistemoms per 16 val., trečiosios kategorijos informacinėms sistemoms – per 8 val., antrosios kategorijos informacinėms sistemoms – per 1 val., pirmosios kategorijos informacinėms sistemoms – per 15 min.;

3.9. reikalavimai informacinės sistemos įrangai ir patalpoms:

3.9.1. pagrindinė informacinės sistemos kompiuterinė įranga turi turėti įtampos filtrą arba (ir) rezervinį maitinimo šaltinį;

3.9.2. turi būti naudojamos kenksmingosios informacinės sistemos programinės įrangos aptikimo priemonės, kurios turi būti reguliariai atnaujinamos;

3.9.3. turi būti operatyviai įdiegiami informacinės sistemos operacinės sistemos ir naudojamos programinės įrangos gamintojų rekomenduojami atnaujinimai;

3.9.4. informacinėje sistemoje turi būti naudojama tik legali programinė įranga;

3.9.5. įranga turi būti prižiūrima laikantis gamintojo rekomendacijų;

3.9.6. įrangos priežiūrą ir gedimų šalinimą turi atlikti kvalifikuoti specialistai;

3.9.7. turi būti apribota fizinė prieiga prie informacinės sistemos tarnybinių stočių (atskiros rakinamos patalpos arba rakinama spinta);

3.9.8. patalpose, kuriose yra informacinės sistemos tarnybinės stotys, turi būti įrengti gaisro ir įsilaužimo davikliai, prijungti prie pastato signalizacijos ir apsaugos tarnybų;

3.9.9. turi būti užtikrintas informacinės sistemos prieinamumas ketvirtosios kategorijos informacinėms sistemoms ne mažiau kaip 70 proc. laiko darbo metu darbo dienomis, trečiosios kategorijos informacinėms sistemoms – ne mažiau kaip 90 proc. laiko darbo metu darbo dienomis, antrosios kategorijos informacinėms sistemoms – ne mažiau kaip 96 proc. laiko visą parą, pirmosios kategorijos informacinėms sistemoms – ne mažiau kaip 99 proc. laiko visą parą;

3.9.10. turi būti daromos atsarginės elektroninės informacijos kopijos (toliau – kopijos), kurios turi būti laikomos atskiroje patalpoje;

3.9.11. informacinės sistemos elektroninės informacijos perdavimo tinklas turi būti atskirtas nuo viešųjų telekomunikacinių tinklų naudojant užkardą ar kitas priemones.

4. Trečiosios kategorijos informacinių sistemų elektroninės informacijos papildomi techniniai saugos reikalavimai:

4.1. atitikties vertinimas turi būti atliekamas ne rečiau kaip kartą per dvejus metus, jei teisės aktuose nenustatyta kitaip;

4.2. informacinė sistema turi perspėti administratorių, kai pagrindinėje informacinės sistemos kompiuterinėje įrangoje sumažėja iki nustatytos pavojingos ribos laisvos kompiuterio atminties ar vietos diske, ilgą laiką stipriai apkraunamas centrinis procesorius ar kompiuterių tinklo sąsaja;

4.3. viešaisiais telekomunikaciniais tinklais perduodamos informacinės sistemos elektroninės informacijos konfidencialumas turi būti užtikrintas, naudojant šifravimą, virtualų privatų tinklą (angl. *virtual private network),* skirtines linijas, saugų valstybinį duomenų perdavimo tinklą ar kitas priemones;

4.4. informacinė sistema turi turėti įvestos elektroninės informacijos tikslumo, užbaigtumo ir patikimumo tikrinimo priemones;

4.5. informacinėje sistemoje turi būti registruojami ir nustatytą laiką saugomi duomenys apie informacinės sistemos įjungimą, išjungimą, sėkmingus ir nesėkmingus bandymus registruotis informacinėje sistemoje, kitus saugai svarbius įvykius, nurodant informacinės sistemos naudotojo identifikatorių ir įvykio laiką; ši informacija turi būti reguliariai analizuojama;

4.6. patekimas į informacinės sistemos tarnybinių stočių patalpas turi būti kontroliuojamas;

4.7. rezervinis maitinimo šaltinis turi užtikrinti informacinės sistemos pagrindinės kompiuterinės įrangos veikimą ne mažiau nei 10 min.;

4.8. jei informacinės sistemos tarnybinių stočių patalpose esančios įrangos bendras galingumas yra daugiau nei 10 kilovatų, turi būti įrengta oro kondicionavimo įranga;

4.9. institucija turi numatyti atsargines patalpas, į kurias galėtų laikinai perkelti informacinės sistemos įrangą, nesant galimybių tęsti veiklą pagrindinėse patalpose; institucijos informacinės sistemos veiklos tęstinumo valdymo planas turi užtikrinti informacinės sistemos veiklos atnaujinimą atsarginėse patalpose per tokį laikotarpį, kad nebūtų nusižengta institucijos įsipareigojimams, susijusiems su informacinės sistemos veikla;

4.10. kopijų darymas turi būti fiksuojamas žurnale;

4.11. kopijos turi būti saugomos užrakintoje nedegioje spintoje;

4.12. elektroninė informacija kopijose turi būti užšifruota arba turi būti imtasi kitų priemonių, neleidžiančių panaudoti kopijų neteisėtam elektroninės informacijos atkūrimui;

4.13. periodiškai turi būti atliekami elektroninės informacijos atkūrimo iš kopijų bandymai;

4.14. atsarginės laikmenos su programine įranga turi būti laikomos nedegioje spintoje;

4.15. slaptažodis turi būti keičiamas ne rečiau kaip kas 6 mėnesius;

4.16. slaptažodį turi sudaryti ne mažiau kaip 6 simboliai;

4.17. slaptažodis turi būti sudarytas iš raidžių, skaičių ir specialiųjų simbolių;

4.18. keičiant slaptažodį informacinė sistema neturi leisti nustatyti slaptažodžio iš buvusių 3 paskutinių slaptažodžių;

4.19. slaptažodžiams neturi būti naudojama asmeninio pobūdžio informacija;

4.20. pirmojo prisijungimo prie informacinės sistemos metu iš informacinės sistemos naudotojo turi būti reikalaujama, kad jis pakeistų slaptažodį;

4.21. turi būti draudžiama slaptažodžius atskleisti tretiesiems asmenims.

5. Antrosios kategorijos informacinių sistemų elektroninės informacijos papildomi techniniai saugos reikalavimai:

5.1. šių reikalavimų 4 punkte nurodyti techniniai saugos reikalavimai;

5.2. atitikties vertinimas turi būti atliekamas ne rečiau kaip kartą per metus, jei teisės aktuose nenustatyta kitaip;

5.3. turi būti reglamentuota nešiojamųjų kompiuterių, skirtų informacinės sistemos elektroninės informacijos tvarkymui, naudojimo ne institucijos patalpose tvarka;

5.4. svarbiausia kompiuterinė įranga ir duomenų perdavimo tinklo mazgai turi turėti rezervinį maitinimo šaltinį, užtikrinantį šios įrangos veikimą ne mažiau kaip 30 min.;

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

5.6. kompiuterinės įrangos gedimai turi būti registruojami žurnale;

5.7. kompiuterinėse darbo vietose turi būti naudojamos centralizuotai valdomos kenksmingosios programinės įrangos aptikimo priemonės, kurios turi būti reguliariai atnaujinamos;

5.8. programinės įrangos diegimą turi atlikti tik įgalioti asmenys;

5.9. programinės įrangos testavimas turi būti atliekamas naudojant atskirą tam skirtą testavimo aplinką;

5.10. informacinė sistema turi registruoti visus elektroninės informacijos pakeitimus, juos atlikusį naudotoją ir pakeitimų atlikimo laiką;

5.11. tarnybinių stočių įvykių žurnaluose (angl. *event log)* turi būti registruojami ir nustatytą laiką saugomi duomenys apie: įjungimą, išjungimą, sėkmingus ir nesėkmingus bandymus registruotis informacinėje sistemoje, bandymus prieiti prie informacinių išteklių, kitus svarbius saugai įvykius, nurodant informacinės sistemos naudotojo identifikatorių ir įvykio laiką, ši informacija turi būti reguliariai analizuojama;

5.12. patekimas į tarnybinių stočių patalpas turi būti registruojamas;

5.13. tarnybinių stočių patalpų durys turi būti šarvuotos ir apsaugotos bent dviem skirtingos konstrukcijos spynomis;

5.14. tarnybinių stočių patalpose turi būti oro kondicionavimo ir drėgmės kontrolės įranga;

5.15. visose patalpose turi būti įrengti gaisro ir įsilaužimo davikliai, prijungti prie pastato signalizacijos ir apsaugos tarnybų;

5.16. patekimas prie darbo vietų turi būti kontroliuojamas;

5.17. atsarginės patalpos turėtų tenkinti pagrindinėms patalpoms keliamus reikalavimus arba institucijos informacinės sistemos veiklos tęstinumo valdymo planas turi nustatyti, kaip per minimalų laikotarpį pasiekti šių reikalavimų atitiktį;

5.18. kopijos turi būti saugomos užrakintoje nedegioje spintoje, kitose patalpose, nei yra įrenginys, kurio elektroninė informacija buvo nukopijuota, arba kitame pastate;

5.19. patekimas į patalpas, kuriose laikomos kopijos, turi būti registruojamas žurnale;

5.20. slaptažodis turi būti keičiamas ne rečiau kaip kas 3 mėnesius;

5.21. slaptažodį turi sudaryti ne mažiau kaip 8 simboliai;

5.22. keičiant slaptažodį informacinė sistema neturi leisti nustatyti slaptažodžio iš buvusių 6 paskutinių slaptažodžių;

5.23. administratorius savo tapatybę turi patvirtinti slaptažodžiu, kuriam keliami aukštesni reikalavimai negu naudotojų slaptažodžiams, arba kitomis autentiškumo patvirtinimo priemonėmis (pvz., biometrinėmis, lustinėmis kortelėmis ir pan.).

6. Pirmosios kategorijos informacinių sistemų elektroninės informacijos papildomi techniniai saugos reikalavimai:

6.1. šių reikalavimų 5 punkte nurodyti techniniai saugos reikalavimai;

6.2. institucija turi įgyvendinti Lietuvos standarte LST ISO/IEC 17799:2006 nurodytas technines saugos priemones, išskyrus priemones, kurios netaikytinos dėl institucijos veiklos, informacinės sistemos ar naudojamos informacinėje sistemoje techninės įrangos pobūdžio;

6.3. atliekant atitikties vertinimą, turi būti atliekamas atitikties reikalavimų 6.2 punkte nurodytiems reikalavimams vertinimas, kurį turi atlikti nepriklausomi specialistai.

III. BAIGIAMOSIOS NUOSTATOS

7. Institucijos privalo užtikrinti saugos priemonių, skirtų ne žemesnei kategorijai, negu yra suteikta jų informacinei sistemai, taikymą. Institucijos gali taikyti saugos priemones, nustatytas aukštesnės kategorijos informacinėms sistemoms ar nenurodytas reikalavimuose.

_____