LIETUVOS RESPUBLIKOS VIDAUS REIKALŲ MINISTRAS

Į S A K Y M A S
DĖL SAUGOS DOKUMENTŲ TURINIO GAIRIŲ PATVIRTINIMO

2007 m. gegužės 8 d. Nr. 1V-172
Vilnius

Įgyvendindamas Elektroninės informacijos saugos valstybės institucijų informacinėse sistemose valstybinės strategijos iki 2008 metų įgyvendinimo priemonių plano, patvirtinto Lietuvos Respublikos Vyriausybės 2006 m. birželio 19 d. nutarimu Nr. 601 (Žin., 2006, Nr. 70-2575), 2.2.1 punktą ir 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), 6 punktu:

1. T v i r t i n u Saugos dokumentų turinio gaires (pridedama).

2. P r i p a ž į s t u netekusiu galios Lietuvos Respublikos vidaus reikalų ministro 2003 m. liepos 16 d. įsakymą Nr. 1V-272 „Dėl Tipinių duomenų saugos nuostatų patvirtinimo“ (Žin., 2003, Nr. 76-3511).

3. N u s t a t a u, kad šis įsakymas įsigalioja nuo 2007 m. birželio 30 d.

VIDAUS REIKALŲ MINISTRAS RAIMONDAS ŠUKYS

_____

PATVIRTINTA

Lietuvos Respublikos vidaus reikalų ministro
2007 m. gegužės 8 d. įsakymu Nr. 1V-172

SAUGOS DOKUMENTŲ TURINIO GAIRĖS

I. BENDROSIOS NUOSTATOS

1. Saugos dokumentų turinio gairėse (toliau – gairės) nustatomas Informacinės sistemos duomenų saugos nuostatų, Saugaus elektroninės informacijos tvarkymo taisyklių, Informacinės sistemos veiklos tęstinumo valdymo plano ir Informacinės sistemos naudotojų administravimo taisyklių (toliau – saugos dokumentai) turinys.

2. Gairėse vartojamos sąvokos

Administratorius – valstybės tarnautojas ar darbuotojas, dirbantis pagal darbo sutartį, atliekantis valstybės informacinės sistemos, valstybės ar žinybinio registro ar kitos informacinės sistemos (toliau – informacinė sistema) priežiūrą.

Elektroninės informacijos saugos incidentas – įvykis ar veiksmas, kuris gali sudaryti neteisėto prisijungimo prie informacinės sistemos galimybę, sutrikdyti ar pakeisti informacinės sistemos veiklą, sunaikinti, sugadinti ar pakeisti elektroninę informaciją, panaikinti ar apriboti galimybę naudotis elektronine informacija, sudaryti sąlygas neleistinai elektroninę informaciją pasisavinti, paskleisti ar kitaip panaudoti.

Informacinės sistemos naudotojas – valstybės tarnautojas ar darbuotojas, dirbantis pagal darbo sutartį, turintis teisę naudotis informacinės sistemos ištekliais numatytoms funkcijoms atlikti.

Saugos įgaliotinis – valstybės institucijos ar įstaigos vadovo paskirtas valstybės tarnautojas arba darbuotojas, dirbantis pagal darbo sutartį, įgyvendinantis elektroninės informacijos saugą informacinėse sistemose.

Kitos gairėse vartojamos sąvokos atitinka sąvokas, nustatytas Lietuvos Respublikos įstatymuose ir kituose teisės aktuose bei Lietuvos standartuose LST ISO/IEC 17799: 2006 ir LST ISO/IEC 27001: 2006.

II. REIKALAVIMAI INFORMACINĖS SISTEMOS DUOMENŲ SAUGOS NUOSTATŲ TURINIUI

3. Informacinės sistemos duomenų saugos nuostatus (toliau – nuostatai) sudaro šie skyriai:

3.1. „Bendrosios nuostatos“, kuriame turi būti nurodyta:

3.1.1. elektroninės informacijos saugumo tikslai, svarba ir esama padėtis;

3.1.2. elektroninės informacijos saugumo užtikrinimo prioritetinės kryptys;

3.1.3. informacinės sistemos valdytojo ir tvarkytojo (tvarkytojų) bei kitų subjektų, kuriems taikomi nuostatų reikalavimai, pavadinimai ir adresai;

3.1.4. informacinės sistemos valdytojo ir tvarkytojo (tvarkytojų) vadovų, saugos įgaliotinio, administratoriaus funkcijos ir atsakomybė;

3.1.5. teisės aktų, kuriais vadovaujamasi tvarkant informacinės sistemos ir šioje sistemoje tvarkomus duomenis (toliau – duomenys) ir užtikrinant jų saugumą, sąrašas.

3.2. „Elektroninės informacijos saugos valdymas“, kuriame turi būti nurodyta:

3.2.1. elektroninės informacijos priskyrimo atitinkamai kategorijai bendrieji reikalavimai, siekiant nustatyti šios informacijos apsaugos poreikį, prioritetus ir lygį;

3.2.2. pagrindinės informacinės sistemos valdytojo nuostatos dėl rizikos veiksnių vertinimo, pagrindinių rizikos vertinimo kriterijų apibūdinimas (rizikos veiksnių vertinimo metodika, naudojama rizikos vertinimo programinė įranga, vertinimo periodiškumas, už vertinimo organizavimą atsakingi asmenys, vertinimo apimtis ir kt.);

3.2.3. elektroninės informacijos saugos priemonių parinkimo principai.

3.3. „Organizaciniai ir techniniai reikalavimai“, kuriame turi būti nurodyta:

3.3.1. metodai ir priemonės, kurie taikomi užtikrinant prieigą prie informacinės sistemos, nurodant leistiną šios prieigos laiką ir būdą;

3.3.2. programinės įrangos, skirtos apsaugoti informacinę sistemą nuo kenksmingos programinės įrangos (virusų, programinės įrangos, skirtos šnipinėjimui, nepageidaujamo elektroninio pašto ir pan.), naudojimo nuostatos ir jos atnaujinimo reikalavimai, nurodant ilgiausią leistiną neatnaujinimo laiką;

3.3.3. programinės įrangos naudojimo nuostatos, ribojančios programinės įrangos, nesusijusios su institucijos ar įstaigos (toliau – institucija) veikla ar informacinės sistemos naudotojo funkcijomis (žaidimai, bylų siuntimo, internetinių pokalbių programos ir kt.), naudojimą;

3.3.4. kompiuterių tinklo filtravimo įrangos (užkardų, turinio kontrolės sistemų, įgaliotųjų serverių (angl. *proxy*) ir kt.) pagrindinės naudojimo nuostatos, už šios įrangos administravimą ir priežiūrą atsakingi asmenys;

3.3.5. leistinos kompiuterių (ypač nešiojamųjų) naudojimo ribos (jei kompiuterius leidžiama naudoti nustatytoms funkcijoms vykdyti ne institucijos patalpose, turi būti nurodytos papildomos saugos priemonės, taikytinos tokiems kompiuteriams (šifravimas, papildomas tapatybės patvirtinimas, prisijungimo ribojimai, rakinimo įrenginių naudojimas ir pan.);

3.3.6. metodai, kurie leidžiami užtikrinant saugų elektroninės informacijos teikimą ir (ar) gavimą (nurodant nuotolinio prisijungimo prie informacinės sistemos būdą, protokolą, duomenų keitimosi formatus, šifravimo, duomenų kopijų skaičiaus reikalavimus, reikalavimą teikti ir (ar) gauti duomenis automatiniu būdu tik pagal duomenų teikimo sutartyse nustatytas specifikacijas ir sąlygas ir t. t.);

3.3.7. pagrindiniai atsarginių duomenų kopijų darymo ir atkūrimo reikalavimai.

3.4. „Reikalavimai personalui“, kuriame turi būti nurodyta:

3.4.1. kvalifikaciniai reikalavimai informacinės sistemos valdytojo ir tvarkytojo personalui;

3.4.2. informacinės sistemos naudotojų mokymo, mokymų dažnumo reikalavimai ir asmuo, atsakingas už šių mokymų organizavimą.

3.5. „Informacinės sistemos naudotojų supažindinimo su saugos dokumentais principai“, kuriame turi būti nurodyti supažindinimo su saugos dokumentais, kitais teisės aktais, kuriais vadovaujamasi tvarkant elektroninę informaciją, užtikrinant jos saugumą, ir atsakomybe už saugos dokumentų nuostatų pažeidimus pagrindiniai reikalavimai bei asmuo, atsakingas už tokio supažindinimo vykdymą.

III. REIKALAVIMAI SAUGAUS ELEKTRONINĖS INFORMACIJOS TVARKYMO TAISYKLIŲ TURINIUI

4. Saugaus elektroninės informacijos tvarkymo taisykles sudaro šie skyriai:

4.1. „Bendrosios nuostatos“, kuriame turi būti nurodyta:

4.1.1. informacinėje sistemoje esančios elektroninės informacijos kategorijų sąrašas;

4.1.2. elektroninės informacijos, priskirtos tam tikrai kategorijai, sąrašas ir asmenys, atsakingi už šios informacijos tvarkymą.

4.2. „Techninių ir kitų saugos priemonių aprašymas“, kuriame turi būti nurodyta:

4.2.1. kompiuterinės įrangos saugos priemonės;

4.2.2. sisteminės ir taikomosios programinės įrangos saugos priemonės;

4.2.3. duomenų perdavimo tinklais saugumo užtikrinimo priemonės;

4.2.4. patalpų ir aplinkos saugumo užtikrinimo priemonės (įėjimo kontrolė, elektros tiekimas, aplinkos drėgnumas, darbo vietos temperatūra, priešgaisrinė sauga);

4.2.5. informacinės sistemos darbo apskaitos ir kitos priemonės, naudojamos užtikrinti elektroninės informacijos saugą.

4.3. „Saugus elektroninės informacijos tvarkymas“, kuriame turi būti nurodyta:

4.3.1. duomenų keitimo, atnaujinimo, įvedimo ir naikinimo tvarka;

4.3.2. informacinės sistemos naudotojo veiksmų registravimo tvarka;

4.3.3. atsarginių duomenų kopijų darymo, saugojimo ir duomenų atkūrimo iš atsarginių

duomenų kopijų tvarka, nurodant kopijuojamų duomenų imtį, atsarginių duomenų kopijų darymo metodus ir dažnumą, visiško ir dalinio duomenų atkūrimo bandymų metodus ir dažnumą bei atsakingus už atsarginių duomenų kopijų darymą, duomenų atkūrimą ir atsarginių duomenų kopijų apsaugą asmenis ir atsarginių duomenų kopijų saugojimo kontrolę;

4.3.4. duomenų perkėlimo ir teikimo kitoms informacinėms sistemoms, duomenų gavimo iš jų tvarka;

4.3.5. duomenų neteisėto kopijavimo, keitimo, naikinimo ar perdavimo nustatymo tvarka;

4.3.6. programinės ir techninės įrangos keitimo ir atnaujinimo tvarka.

4.4. „Reikalavimai, keliami informacinių sistemų funkcionavimui reikalingoms paslaugoms ir jų teikėjams“, kuriame turi būti nurodyta:

4.4.1. paslaugų teikėjų prieigos prie informacinės sistemos lygiai ir sąlygos;

4.4.2. reikalavimai, keliami patalpoms, įrangai, informacinių sistemų priežiūrai, duomenų perdavimui tinklais ir kitoms paslaugoms.

IV. REIKALAVIMAI INFORMACINĖS SISTEMOS VEIKLOS TĘSTINUMO VALDYMO PLANO TURINIUI

5. Informacinės sistemos veiklos tęstinumo valdymo planą (toliau – planas) sudaro šie skyriai:

5.1. „Bendrosios nuostatos“, kuriame turi būti nurodyta:

5.1.1. plano įsigaliojimo tvarka;

5.1.2. saugos įgaliotinio, administratorių, informacinės sistemos naudotojų funkcijos, įgaliojimai ir veiksmai pagal planą;

5.1.3. nuostata, kad planas privalomas visiems informacinės sistemos naudotojams ir turi būti parengtas kiekvienam pastatui, kuriame tvarkomi institucijos informacinės sistemos duomenys;

5.1.4. finansinių ir kitokių išteklių, numatomų informacinės sistemos veiklai atkurti įvykus elektroninės informacijos saugos incidentui, šaltiniai;

5.1.5. informacinės sistemos veiklos kriterijai, pagal kuriuos galima nustatyti, ar informacinės sistemos veikla yra atkurta.

5.2. „Organizacinės nuostatos“, kuriame turi būti nurodyta:

5.2.1. informacinės sistemos veiklos tęstinumo valdymo grupės (toliau – veiklos tęstinumo valdymo grupė) sudėtis (vadovas, ne mažiau kaip du jo pavaduotojai ir kiti nariai);

5.2.2. veiklos tęstinumo valdymo grupės funkcijos:

5.2.2.1. situacijos analizė ir sprendimų informacinės sistemos veiklos tęstinumo valdymo klausimais priėmimas;

5.2.2.2. bendravimas su viešosios informacijos rengėjų ir viešosios informacijos skleidėjų atstovais;

5.2.2.3. bendravimas su kitų informacinių sistemų veiklos tęstinumo valdymo grupėmis;

5.2.2.4. bendravimas su teisėsaugos ir kitomis institucijomis, institucijos darbuotojais ir kitomis interesų grupėmis;

5.2.2.5. finansinių ir kitų išteklių, reikalingų informacinės sistemos veiklai atkurti, įvykus elektroninės informacijos saugos incidentui, naudojimo kontrolė;

5.2.2.6. elektroninės informacijos fizinė sauga įvykus elektroninės informacijos saugos incidentui;

5.2.2.7. logistika (žmonių, daiktų, įrangos gabenimas ir jo organizavimas);

5.2.2.8. kitos veiklos tęstinumo valdymo grupei pavestos funkcijos;

5.2.3. informacinės sistemos veiklos atkūrimo grupės (toliau – veiklos atkūrimo grupė) sudėtis (vadovas, pavaduotojas ir kiti nariai, nurodant asmenis, atsakingus už atskirų funkcijų vykdymą, ne mažiau kaip du kiekvienai funkcijai);

5.2.4. veiklos atkūrimo grupės funkcijos:

5.2.4.1. informacinės sistemos veiklos atkūrimo priežiūra ir koordinavimas;

5.2.4.2. tarnybinių stočių veikimo atkūrimo organizavimas;

5.2.4.3. kompiuterių tinklo veikimo atkūrimo organizavimas;

5.2.4.4. informacinės sistemos duomenų atkūrimo organizavimas;

5.2.4.5. taikomųjų programų tinkamo veikimo atkūrimo organizavimas;

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

5.2.4.7. kitos veiklos atkūrimo grupei pavestos funkcijos;

5.2.5. veiklos tęstinumo valdymo grupės ir veiklos atkūrimo grupės komunikavimo būdai ir dažnumas;

5.2.6. informacinės sistemos veiklos atkūrimo detalusis planas;

5.2.7. įrangos, reikalingos pakeisti elektroninės informacijos saugos incidento metu sunaikintą įrangą, įsigijimo tvarka;

5.2.8. bendravimo veiklos tęstinumo valdymo grupėje ir veiklos atkūrimo grupėje būdas (el. paštas, mobilusis ryšys ir kt.);

5.2.9. reikalavimai, keliami atsarginėms patalpoms, naudojamoms informacinės sistemos veiklai atkurti elektroninės informacijos saugos incidento atveju.

5.3. „Aprašomosios nuostatos“, kuriame turi būti nurodyta:

5.3.1. informacinių technologijų įrangos sąrašai, šios įrangos parametrai ir už šios įrangos priežiūrą atsakingi administratoriai bei minimalus informacinės sistemos veiklos atkūrimui, nesant administratoriaus, reikalingos kompetencijos ar žinių lygis;

5.3.2. minimalaus funkcionalumo informacinių technologijų įrangos, tinkamos užtikrinti institucijos poreikius atitinkančią informacinės sistemos veiklą elektroninės informacijos saugos incidento metu, specifikacija;

5.3.3. kiekvieno pastato aukšto patalpų brėžiniai ir šiose patalpose esanti įranga bei komunikacijos:

5.3.3.1. tarnybinės stotys;

5.3.3.2. duomenų perdavimo įranga (šakotuvai, skirstytuvai, kelvedžiai, modemai, telefonų stotys ir kt.);

5.3.3.3. kompiuterių tinklo ir telefoninio tinklo mazgai;

5.3.3.4. duomenų laidų vedimo tarp pastato aukštų vietos;

5.3.3.5. elektros įvedimo pastate vietos;

5.3.4. kompiuterių tinklo fizinio ir loginio sujungimo schemos;

5.3.5. atsarginių patalpų, naudojamų informacinės sistemos veiklai atkurti elektroninės informacijos saugos incidento atveju, adresas ir būdai, kaip iki jų nuvykti;

5.3.6. duomenų teikimo bei kompiuterinės, techninės ir programinės įrangos priežiūros sutarčių sąrašai;

5.3.7. programinės įrangos laikmenų ir laikmenų su atsarginėmis duomenų kopijomis saugojimo vieta ir šių laikmenų perkėlimo į saugojimo vietą laikas ir sąlygos;

5.3.8. institucijos darbuotojų sąrašas, kuriame nurodyti darbuotojų darbo telefonai, o veiklos tęstinumo valdymo grupės ir veiklos atkūrimo grupės narių – mobiliojo ir namų telefono numeriai ir gyvenamosios vietos adresai.

5.4. „Plano veiksmingumo išbandymo nuostatos“, kuriame turi būti nurodyta:

5.4.1. plano veiksmingumo paskutinio ir kito planuojamo išbandymo būdas ir data;

5.4.2. asmuo, atsakingas už plano veiksmingumo išbandymo metu pastebėtų trūkumų ataskaitos parengimą ir pateikimą informacinės sistemos valdytojui;

5.4.3. plano veiksmingumo išbandymo metu pastebėtų trūkumų šalinimo principai.

V. REIKALAVIMAI INFORMACINĖS SISTEMOS NAUDOTOJŲ ADMINISTRAVIMO TAISYKLIŲ TURINIUI

6. Informacinės sistemos naudotojų administravimo taisykles sudaro šie skyriai:

6.1. „Bendrosios nuostatos“, kuriame turi būti nurodyta:

6.1.1. subjektai, kuriems bus taikomos šios taisyklės;

6.1.2. prieinamumo prie duomenų principai.

6.2. „Informacinės sistemos naudotojų įgaliojimai, teisės ir pareigos“, kuriame turi būti nurodyti informacinės sistemos naudotojų įgaliojimai, teisės ir pareigos renkant, tvarkant, perduodant, saugant, naikinant ar kitaip naudojant elektroninę informaciją.

6.3. „Informacinės sistemos naudotojų supažindinimo su saugos dokumentais tvarka“, kuriame turi būti nurodytas asmuo, atsakingas už informacinės sistemos naudotojų supažindinimą su saugos dokumentais, tokio supažindinimo forma, pakartotinio supažindinimo sąlygos ir kt.

6.4. „Saugaus duomenų teikimo informacinės sistemos naudotojams kontrolės tvarka“, kuriame turi būti nurodyta:

6.4.1. tvarka, kuri bus taikoma registruojant ir išregistruojant informacinės sistemos naudotojus, ir už šių veiksmų atlikimą atsakingas asmuo;

6.4.2. priemonės, kurios bus taikomos informacinės sistemos naudotojų tapatybei nustatyti;

6.4.3. reikalavimai informacinės sistemos naudotojų slaptažodžių sudarymui, galiojimo trukmei ir keitimui;

6.4.4. sąlygos, kada panaikinama informacinės sistemos naudotojų teisė dirbti su konkrečia elektronine informacija;

6.4.5. leistini nuotolinio informacinės sistemos naudotojų prisijungimo prie informacinės sistemos būdai.

_____