Suvestinė redakcija nuo 2014-05-01

Įsakymas paskelbtas: Žin. 2004, Nr. 144-5270, i. k. 1042020ISAK0004-349

Nauja redakcija nuo 2014-05-01:
Nr. 4-79, 2014-02-05, paskelbta TAR 2014-02-06, i. k. 2014-01211

LIETUVOS RESPUBLIKOS ŪKIO MINISTRAS

ĮSAKYMAS DĖL NACIONALINIAM SAUGUMUI UŽTIKRINTI SVARBIŲ ĮMONIŲ, VEIKIANČIŲ ŪKIO MINISTRUI PAVESTOSE VALDYMO SRITYSE, INFORMACINĖS SAUGOS REIKALAVIMŲ PATVIRTINIMO

2004 m. rugsėjo 22 d. Nr. 4-349
Vilnius

Vadovaudamasis Lietuvos Respublikos Vyriausybės 2004 m. birželio 8 d. nutarimo Nr. 699 „Dėl įgaliojimų suteikimo įgyvendinant Lietuvos Respublikos strateginę reikšmę nacionaliniam saugumui turinčių įmonių ir įrenginių bei kitų nacionaliniam saugumui užtikrinti svarbių įmonių įstatymą“ 2 punktu,

t v i r t i n u Nacionaliniam saugumui užtikrinti svarbių įmonių, veikiančių ūkio ministrui pavestose valdymo srityse, informacinės saugos reikalavimus (pridedama).

ŪKIO MINISTRAS PETRAS ČĖSNA

PATVIRTINTA
Lietuvos Respublikos ūkio ministro
2004 m. rugsėjo 22 d. įsakymu Nr. 4-349
(Lietuvos Respublikos ūkio ministro
2014 m. vasario 5 d. įsakymo Nr. 4-79
redakcija)

NACIONALINIAM SAUGUMUI UŽTIKRINTI SVARBIŲ ĮMONIŲ, VEIKIANČIŲ ŪKIO MINISTRUI PAVESTOSE VALDYMO SRITYSE, INFORMACINĖS SAUGOS REIKALAVIMAI

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Nacionaliniam saugumui užtikrinti svarbių įmonių, veikiančių ūkio ministrui pavestose valdymo srityse, informacinės saugos reikalavimai (toliau – Reikalavimai) nustato Reikalavimų 5 punkte nurodytų įmonių informacinės saugos užtikrinimą ir organizavimą, saugos dokumentų turinį, informacijos saugos techninius reikalavimus, informacinės saugos incidentų valdymą, rizikos įvertinimą, informacinės sistemos pokyčių valdymą, informacinių technologijų ir telekomunikacijų (toliau – ITT) saugos atitikties vertinimą, informacinės sistemos naudotojų atsakomybę.

2. Įmonės informacijos saugos tikslas – užtikrinti saugų ir nenutrūkstamą ITT darbą, apsaugoti įmonės, veikiančios ūkio ministrui pavestose valdymo srityse (toliau – Įmonė), veiklai svarbią informaciją nuo nepageidaujamo išorės poveikio, galinčio ją iškraipyti ar sunaikinti, taip pat nuo nesankcionuoto informacijos, kurią Įmonės valdyba priskyrė komercinei (gamybinei) paslapčiai ir konfidencialiai informacijai (toliau – konfidenciali informacija), atskleidimo, tinkamai aprūpinti informacija darbuotojus ir trečiąsias šalis, jeigu to reikia jų funkcijoms atlikti.

3. Kiekviena nacionaliniam saugumui užtikrinti svarbi Įmonė informacinę saugą organizuoja ir vykdo laikydamasi Lietuvos Respublikos įstatymų, kitų teisės aktų reikalavimų.

4. Reikalavimai nereguliuoja informacijos, pripažintos valstybės ar tarnybos paslaptimi, saugos.

5. Reikalavimai taikomi šioms Įmonėms:

5.1. akcinei bendrovei „Achema“;

5.2. akcinei bendrovei Giraitės ginkluotės gamyklai.

6. Reikalavimuose vartojamos sąvokos:

6.1. **Elektroninė informacija** – Įmonės informacinėje sistemoje tvarkomi duomenys, dokumentai ir informacija.

6.2. **Informacijos konfidencialumas** – informacijos savybė, leidžianti su Įmonės informacija susipažinti tik įgaliotiems asmenims.

6.3. **Informacijos prieinamumas** – informacijos savybė, leidžianti Įmonės informaciją tvarkyti reikiamu metu.

6.4. **Informacijos sauga** – informacijos konfidencialumo, vientisumo ir prieinamumo užtikrinimas.

6.5. **Informacijos saugos incidentas** – įvykis ar veiksmas, galintis sudaryti neteisėto prisijungimo prie Įmonės informacinės sistemos galimybę, sutrikdyti ar pakeisti Įmonės informacinės sistemos veiklą, sunaikinti, sugadinti ar pakeisti informaciją, panaikinti ar apriboti galimybę ja naudotis, sudaryti sąlygas neleistinai ją pasisavinti, atskleisti ar kitaip panaudoti.

6.6. **Informacijos saugos politika** – pagrindiniai Įmonės informacijos saugos užtikrinimo ir valdymo principai, reikalavimai, į kuriuos atsižvelgiant turi būti derinami informacinės veiklos ir naudojimo procesai, procedūros ir rengiami juos reguliuojantys dokumentai. Informacijos saugos politika išdėstoma Įmonės informacinės sistemos saugos nuostatuose (toliau – saugos nuostatai).

6.7. **Informacijos vientisumas** – informacijos savybė, užtikrinanti, kad informacija nebuvo atsitiktinai ar neteisėtai pakeista ar sunaikinta.

6.8. **Informacinės sistemos administratorius** (toliau – administratorius) – Įmonės darbuotojas, prižiūrintis informacinę sistemą ir (arba) jos infrastruktūrą, užtikrinantis jos veikimą ir elektroninės informacijos saugą, ar kitas asmuo, kuriam paslaugų teikimo sutartyje nustatytomis sąlygomis ir tvarka perduotos Įmonės informacinės sistemos ir (arba) jos infrastruktūros priežiūros funkcijos.

6.9. **Informacinės sistemos naudotojas** – Įmonės darbuotojas pagal kompetenciją ar kitas asmuo, pagal susitarimą (sutartį) naudojantis ir (arba) tvarkantis Įmonės elektroninę informaciją.

6.10. **Informacinės sistemos saugos įgaliotinis** (toliau – saugos įgaliotinis) – Įmonės darbuotojas, koordinuojantis ir prižiūrintis informacijos saugos politikos įgyvendinimą informacinėje sistemoje.

6.11. **Trečiosios šalys** – paslaugų teikėjai, partneriai, klientai, kiti asmenys, galintys turėti prieigą prie Įmonės informacinės sistemos.

7. Kitos Reikalavimuose vartojamos sąvokos apibrėžtos Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatyme, kituose teisės aktuose, Lietuvos standartuose LST ISO/IEC 27001:2006, LST ISO/IEC 27002:2009 ir Nacionaliniam saugumui užtikrinti svarbių įmonių, veikiančių ūkio ministrui pavestose valdymo srityse, fizinės saugos reikalavimuose, patvirtintuose Lietuvos Respublikos ūkio ministro 2004 m. rugsėjo 15 d. įsakymu Nr. 4-334 „Dėl Nacionaliniam saugumui užtikrinti svarbių įmonių, veikiančių ūkio ministrui pavestose valdymo srityse, fizinės saugos reikalavimų patvirtinimo“.

II SKYRIUS
INFORMACIJOS SAUGOS UŽTIKRINIMAS

8. Užtikrinant Įmonės informacijos saugą, rekomenduojama vadovautis Lietuvos standartais LST ISO/IEC 27001:2006, LST ISO/IEC 27002:2009, taip pat kitais Lietuvos ir tarptautiniais grupės „Informacijos technologija. Saugumo metodai“ standartais, apibūdinančiais saugų informacijos tvarkymą.

9. Įmonės informacinės saugos valdymas turi būti pagrįstas rizikos vertinimu, t. y. naudojamos saugos priemonės turi atitikti informacijos svarbą ir jai kylančią riziką. Įmonėje nustatomi ir patvirtinami rizikos valdymo organizavimo pagrindai ir atsakomybė, pagrindiniai rizikos identifikavimo, vertinimo, valdymo principai ir procedūros ir pagal juos vertinama rizika.

10. Už Įmonės informacijos saugą atsakingas Įmonės vadovas.

11. Įmonė privalo turėti šiuos Reikalavimų nuostatas atitinkančius dokumentus (toliau – saugos dokumentai):

11.1. saugos nuostatus;

11.2. elektroninės informacijos saugaus tvarkymo taisykles;

11.3. informacinės sistemos veiklos tęstinumo valdymo planą (toliau – planas);

11.4. informacinės sistemos naudotojų administravimo taisykles.

12. Reikalavimų 11.2–11.4 papunkčiuose nurodyti dokumentai turi būti parengti ir patvirtinti ne vėliau kaip per 6 mėnesius nuo saugos nuostatų patvirtinimo dienos.

13. Saugos nuostatuose apibrėžiama informacinės sistemos naudotojų mokymo planavimo, organizavimo ir vykdymo tvarka.

14. Informacinės saugos valdymas Įmonėje turi būti nuolat tobulinamas, periodiškai (ne rečiau kaip vieną kartą per metus) peržiūrimi ir tobulinami saugos dokumentai, atsižvelgiant į besikeičiančius aplinkos veiksnius ir Įmonės informacinės saugos valdymo stebėseną (monitoringą). Įvertinus riziką ar ITT saugos atitiktį arba Įmonėje įvykus esminių organizacinių, sisteminių ar kitokių pokyčių, saugos dokumentai taip pat turi būti peržiūrėti.

15. Įmonės vadovo įsakyme, kuriuo tvirtinami saugos nuostatai, nustatomi Reikalavimų 11.2–11.4 papunkčiuose nurodytų saugos dokumentų rengėjai ir dokumentų parengimo terminai, paskiriamas saugos įgaliotinis, informacinės sistemos administratorius.

III SKYRIUS
REKOMENDUOJAMAS SAUGOS DOKUMENTŲ TURINYS

16. Rekomenduojama, kad saugos nuostatus sudarytų šie skyriai:

16.1. „Bendrosios nuostatos“, kuriame būtų nurodyta:

16.1.1. elektroninės informacijos saugos užtikrinimo prioritetinės kryptys ir tikslai;

16.1.2. Įmonės ir informacinės sistemos tvarkytojo (tvarkytojų), kitų subjektų, kuriems taikomi saugos nuostatų reikalavimai, pavadinimai ir adresai (jeigu dėl didelio skaičiaus ar kitų priežasčių neįmanoma išvardyti visų subjektų, būtina nurodyti jų grupes pagal veiklos ar pavaldumo pobūdį);

16.1.3. Įmonės ir informacinės sistemos tvarkytojo (tvarkytojų), saugos įgaliotinio, administratoriaus funkcijos (jeigu paskiriami keli saugos įgaliotiniai ar administratoriai, turi būti atskirai nurodytos kiekvieno saugos įgaliotinio ir administratoriaus funkcijos);

16.1.4. teisės aktų, kuriais vadovaujamasi tvarkant elektroninę informaciją ir užtikrinant jos saugą, sąrašas;

16.2. „Elektroninės informacijos saugos valdymas“, kuriame būtų nurodyta:

16.2.1. informacinėje sistemoje tvarkomos elektroninės informacijos svarbos kategorija ir jos priskyrimo tam tikrai svarbos kategorijai kriterijai, o jeigu informacinėje sistemoje tvarkoma skirtingos svarbos elektroninė informacija, nurodomos visos elektroninės informacijos svarbos kategorijos ir jos priskyrimo kiekvienai iš svarbos kategorijų kriterijai;

16.2.2. pagrindinės Įmonės nuostatos dėl rizikos veiksnių vertinimo, pagrindinių rizikos vertinimo kriterijų apibūdinimas (rizikos veiksnių vertinimo metodika, naudojami rizikos vertinimo dokumentai (vadovai, brošiūros, klausimynai, rekomendacijos, interaktyvios priemonės (kompiuterinės programos) ir panašiai), vertinimo periodiškumas, vertinimo apimtis ir kita);

16.2.3. elektroninės informacijos saugos priemonių parinkimo principai;

16.3. „Organizaciniai ir techniniai reikalavimai“, kuriame būtų nurodyta:

16.3.1. programinės įrangos, skirtos informacinei sistemai nuo kenksmingos programinės įrangos (virusų, programinės įrangos, skirtos šnipinėti, nepageidaujamo elektroninio pašto ir panašiai) apsaugoti, naudojimo nuostatos ir jos atnaujinimo reikalavimai (nurodomas maksimalus laikas, kurį leidžiama naudoti neatnaujintą šią įrangą);

16.3.2. programinės įrangos, įdiegtos kompiuteriuose ir serveriuose, naudojimo nuostatos;

16.3.3. kompiuterių tinklo filtravimo įrangos (užkardų, turinio kontrolės sistemų, įgaliotųjų serverių (angl. *proxy*) ir kita) pagrindinės naudojimo nuostatos;

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

16.3.5. metodai, kuriais leidžiama užtikrinti saugų elektroninės informacijos teikimą ir (arba) gavimą (nurodomas nuotolinio prisijungimo prie informacinės sistemos būdas, protokolas, elektroninės informacijos keitimosi formatai, šifravimo, elektroninės informacijos kopijų skaičiaus reikalavimai, reikalavimas teikti ir (arba) gauti elektroninę informaciją automatiniu būdu tik pagal duomenų teikimo sutartyse nustatytas specifikacijas ir sąlygas ir panašiai);

16.3.6. pagrindiniai atsarginių elektroninės informacijos kopijų darymo ir atkūrimo reikalavimai;

16.4. „Reikalavimai personalui“, kuriame būtų nurodyta:

16.4.1. informacinės sistemos naudotojų, administratoriaus (administratorių) ir saugos įgaliotinio kvalifikaciniai reikalavimai;

16.4.2. informacinės sistemos naudotojų mokymo planavimo, organizavimo ir vykdymo tvarka, mokymo dažnumo reikalavimai;

16.5. „Informacinės sistemos naudotojų supažindinimo su saugos dokumentais principai“, kuriame būtų nurodyti:

16.5.1. pagrindiniai reikalavimai norint supažindinti (pakartotinai supažindinti) informacinės sistemos naudotojus su:

16.5.1.1. saugos dokumentais ir kitais teisės aktais, kuriais vadovaujamasi tvarkant elektroninę informaciją ir užtikrinant jos saugumą;

16.5.1.2. atsakomybe už saugos dokumentų nuostatų pažeidimus;

16.5.2. būdai, kaip informacinės sistemos naudotojai supažindinami su Reikalavimų 16.5.1.1 papunktyje nurodytais dokumentais ar teisės aktais ir Reikalavimų 16.5.1.2 papunktyje nustatyta atsakomybe.

17. Rekomenduojama, kad elektroninės informacijos saugaus tvarkymo taisykles turėtų sudaryti šie skyriai:

17.1. „Bendrosios nuostatos“, kuriame būtų nurodyta:

17.1.1. informacinėje sistemoje tvarkomos elektroninės informacijos (jos grupių) sąrašas. Jeigu visa tvarkoma elektroninė informacija (jos grupės) nurodyta informacinės sistemos nuostatose, gali būti pateikiamos nuorodos į atitinkamus informacinės sistemos nuostatų punktus (papunkčius), o jeigu informacinėje sistemoje tvarkoma skirtingos svarbos elektroninė informacija, nurodoma atitinkama elektroninės informacijos grupė ir jos svarbos kategorija;

17.1.2. už informacinėje sistemoje tvarkomos elektroninės informacijos (jos grupių), priskirtų tam tikrai elektroninės informacijos svarbos kategorijai, tvarkymą atsakingų informacinės sistemos naudotojų ar informacinės sistemos naudotojų grupių sąrašas;

17.2. „Techninių ir kitų saugos priemonių aprašas“, kuriame būtų nurodyta:

17.2.1. kompiuterinės įrangos saugos priemonės;

17.2.2. sisteminės ir taikomosios programinės įrangos saugos priemonės;

17.2.3. elektroninės informacijos perdavimo tinklais saugos užtikrinimo priemonės;

17.2.4. patalpų ir aplinkos saugos užtikrinimo priemonės (įėjimo kontrolė, elektros tiekimas, aplinkos drėgmė, darbo vietos temperatūra, priešgaisrinė sauga);

17.2.5. kitos priemonės, naudojamos elektroninės informacijos saugai užtikrinti (pavyzdžiui, informacinės sistemos darbo apskaitos priemonės ir panašiai);

17.3. „Saugus elektroninės informacijos tvarkymas“, kuriame būtų nurodyta:

17.3.1. elektroninės informacijos saugaus keitimo, atnaujinimo, įvedimo ir naikinimo užtikrinimo tvarka;

17.3.2. informacinės sistemos naudotojų veiksmų registravimo tvarka;

17.3.3. atsarginių elektroninės informacijos kopijų darymo, saugojimo ir elektroninės informacijos atkūrimo iš atsarginių kopijų tvarka;

17.3.4. saugaus elektroninės informacijos perkėlimo ir teikimo susijusioms informacinėms sistemoms, elektroninės informacijos gavimo iš jų užtikrinimo tvarka;

17.3.5. elektroninės informacijos neteisėto kopijavimo, keitimo, naikinimo ar perdavimo nustatymo tvarka;

17.3.6. programinės ir techninės įrangos keitimo ir atnaujinimo tvarka;

17.3.7. informacinės sistemos pokyčių (toliau – pokyčiai) valdymo tvarka, apimanti šias veiklas:

17.3.7.1. pokyčių nustatymą;

17.3.7.2. pokyčių suskirstymą į kategorijas, atsižvelgiant į pokyčių svarbą, aktualumą, poreikį ir panašiai;

17.3.7.3. pokyčių įtakos vertinimą;

17.3.7.4. pokyčių prioritetų nustatymą;

17.3.7.5. pokyčių atlikimą;

17.3.8. nešiojamųjų kompiuterių ir kitų mobiliųjų įrenginių naudojimo tvarka;

17.4. „Reikalavimai, keliami informacinėms sistemoms funkcionuoti reikalingoms paslaugoms ir jų teikėjams“, kuriame būtų nurodyta:

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

17.4.2. patalpų, įrangos, informacinių sistemų priežiūros, elektroninės informacijos perdavimo tinklais ir kitų paslaugų reikalavimai.

18. Rekomenduojama, kad planą sudarytų šie skyriai:

18.1. „Bendrosios nuostatos“, kuriame būtų nurodyta:

18.1.1. plano įsigaliojimo laikas (įvykus elektroninės informacijos saugos incidentui);

18.1.2. saugos įgaliotinio, administratoriaus (administratorių), informacinės sistemos naudotojų ir kitų asmenų įgaliojimai ir veiksmai pagal planą, įvykus elektroninės informacijos saugos incidentui;

18.1.3. plano privalomumas informacinės sistemos tvarkytojams, saugos įgaliotiniui, administratoriui (administratoriams) ir informacinės sistemos naudotojams;

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

18.1.5. informacinės sistemos veiklos kriterijai, pagal kuriuos galima nustatyti, ar informacinės sistemos veikla atkurta;

18.2. „Organizacinės nuostatos“, kuriame būtų nurodyta:

18.2.1. informacinės sistemos veiklos tęstinumo valdymo grupės (toliau – veiklos tęstinumo valdymo grupė) sudėtis (vadovas, pavaduotojas, nariai);

18.2.2. veiklos tęstinumo valdymo grupės funkcijos:

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

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

18.2.2.3. bendravimas su susijusių informacinių sistemų veiklos tęstinumo valdymo grupėmis;

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

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

18.2.2.6. elektroninės informacijos fizinė sauga, įvykus elektroninės informacijos saugos incidentui;

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

18.2.2.8. informacinės sistemos veiklos atkūrimo priežiūra ir koordinavimas;

18.2.2.9. kitos veiklos tęstinumo valdymo grupei pavestos funkcijos;

18.2.3. informacinės sistemos veiklos atkūrimo grupės (toliau – veiklos atkūrimo grupė) vadovas, pavaduotojas ir nariai (nurodomos ne mažiau kaip 2 pareigybės asmenų, atsakingų už kiekvienos iš funkcijų atlikimą); į veiklos atkūrimo grupę neturėtų būti įtraukiami asmenys, esantys veiklos tęstinumo valdymo grupėje, išskyrus išimtinius atvejus, kai nepakanka žmogiškųjų išteklių veiklos atkūrimo grupei sudaryti;

18.2.4. veiklos atkūrimo grupės funkcijos:

18.2.4.1. tarnybinių stočių veikimo atkūrimo organizavimas;

18.2.4.2. kompiuterių tinklo veikimo atkūrimo organizavimas;

18.2.4.3. informacinės sistemos elektroninės informacijos atkūrimo organizavimas;

18.2.4.4. taikomųjų programų tinkamo veikimo atkūrimo organizavimas;

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

18.2.4.6. kitos veiklos atkūrimo grupei pavestos funkcijos;

18.2.5. informacinės sistemos veiklos atkūrimo detalusis planas, kuriame nurodytas veiksmų vykdymo eiliškumas, terminai, atsakingi vykdytojai (rekomenduojama numatyti atskirus plano scenarijus informacinės sistemos veiklai atkurti po skirtingo pobūdžio ir masto elektroninės informacijos saugos incidentų);

18.2.6. atsarginių patalpų, naudojamų informacinės sistemos veiklai atkurti, kai įvyksta elektroninės informacijos saugos incidentas, reikalavimai, atsarginių patalpų adresas ir būdai, kaip iki jų nuvykti;

18.2.7. veiklos tęstinumo valdymo grupės ir veiklos atkūrimo valdymo grupės bendradarbiavimo reikalavimai (dažnis, formos ir kita);

18.3. „Aprašomosios nuostatos“, kuriame būtų nurodyta:

18.3.1. parengtų ir saugomų dokumentų sąrašas:

18.3.1.1. dokumentas, kuriame nurodyti informacinių technologijų įrangos parametrai ir už šios įrangos priežiūrą atsakingas administratorius (administratoriai), taip pat reikiamos kompetencijos ar žinių lygis minimaliai informacinės sistemos veiklai atkurti tuo atveju, jei administratorius dėl komandiruotės, ligos ar kitų priežasčių negali operatyviai atvykti į darbo vietą;

18.3.1.2. dokumentas, kuriame nurodyta minimalaus funkcionalumo informacinių technologijų įrangos, tinkamos institucijos poreikius atitinkančiai informacinės sistemos veiklai užtikrinti, įvykus elektroninės informacijos saugos incidentui, specifikacija;

18.3.1.3. dokumentas, kuriame nurodyti kiekvieno pastato, kuriame yra informacinės sistemos įranga, aukšto patalpų brėžiniai ir juose pažymėti:

18.3.1.3.1. tarnybinės stotys;

18.3.1.3.2. kompiuterių tinklo ir telefonų tinklo mazgai;

18.3.1.3.3. kompiuterių tinklo ir telefonų tinklo laidų vedimo tarp pastato aukštų vietos;

18.3.1.3.4. elektros įvado pastate vietos;

18.3.1.4. dokumentas, kuriame nurodytos kompiuterių tinklo fizinio ir loginio sujungimo schemos;

18.3.1.5. dokumentas, kuriame nurodytos elektroninės informacijos teikimo ir kompiuterinės, techninės ir programinės įrangos priežiūros sutartys, atsakingų už šių sutarčių įgyvendinimo priežiūrą asmenų pareigos;

18.3.1.6. dokumentas, kuriame nurodyta programinės įrangos laikmenų ir laikmenų su atsarginėmis elektroninės informacijos kopijomis saugojimo vieta ir šių laikmenų perkėlimo į saugojimo vietą laikas ir sąlygos;

18.3.1.7. dokumentas, kuriame nurodytas veiklos tęstinumo valdymo grupės ir veiklos atkūrimo grupės narių sąrašas su kontaktiniais duomenimis, leidžiančiais pasiekti šiuos asmenis bet kuriuo metu;

18.3.2. už Reikalavimų 18.3.1 papunktyje nurodytų dokumentų parengimą atsakingo asmens pareigos;

18.3.3. už Reikalavimų 18.3.1 papunktyje nurodytų dokumentų saugojimą atsakingas administratorius (administratoriai);

18.3.4. jeigu Įmonė naudoja (pagal nuomos, panaudos ar kitas sutartis) visą informacinės sistemos techninę įrangą ar jos dalį, priklausančias ir esančias trečiosios šalies patalpose, – sutarties su trečiąja šalimi data ir numeris; sutarties kopiją turi saugoti administratorius (administratoriai).

18.4. „Plano veiksmingumo išbandymo nuostatos“, kuriame būtų nurodyta:

18.4.1. plano veiksmingumo paskutinio ir kito planuojamo išbandymo būdas ir periodiškumas;

18.4.2. asmuo, atsakingas už išbandant plano veiksmingumą pastebėtų trūkumų ataskaitos parengimą ir pateikimą Įmonei;

18.4.3. išbandant plano veiksmingumą pastebėtų trūkumų šalinimo principai.

19. Rekomenduojama, kad informacinės sistemos naudotojų administravimo taisykles sudarytų šie skyriai:

19.1. „Bendrosios nuostatos“, kuriame būtų nurodyta:

19.1.1. subjektai, kuriems bus taikomos šios taisyklės;

19.1.2. prieigos prie elektroninės informacijos principai;

19.2. „Informacinės sistemos naudotojų ir administratorių įgaliojimai, teisės ir pareigos“, kuriame būtų nurodyta:

19.2.1. informacinės sistemos naudotojų įgaliojimai, teisės ir pareigos tvarkant elektroninę informaciją;

19.2.2. informacinės sistemos administratoriaus (administratorių) prieigos prie informacinės sistemos lygiai ir jiems taikomi elektroninės informacijos saugos reikalavimai (elektroninės informacijos skaitymas, kūrimas, atnaujinimas, naikinimas, informacinės sistemos naudotojų informacijos, prieigos teisių redagavimas ir panašiai);

19.3. „Saugaus elektroninės informacijos teikimo informacinės sistemos naudotojams kontrolės tvarka“, kuriame būtų nurodyta:

19.3.1. tvarka, pagal kurią bus registruojami ir išregistruojami informacinės sistemos naudotojai, ir už tai atsakingas asmuo;

19.3.2. informacinės sistemos naudotojų tapatybės nustatymo priemonės;

19.3.3. informacinės sistemos naudotojų slaptažodžių sudarymo, galiojimo trukmės ir keitimo reikalavimai;

19.3.4. sąlygos ir atvejai, kai panaikinama informacinės sistemos naudotojų teisė dirbti su konkrečia elektronine informacija;

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

IV SKYRIUS
INFORMACINĖS SAUGOS ORGANIZAVIMAS

20. Saugos įgaliotiniu neturėtų būti skiriamas asmuo, turintis neišnykusį ar nepanaikintą teistumą už nusikaltimą elektroninių duomenų ir informacinių sistemų saugumui, taip pat paskirtą administracinę nuobaudą už neteisėtą asmens duomenų tvarkymą ir privatumo apsaugos pažeidimą elektroninių ryšių srityje, elektroninių ryšių išteklių naudojimo ir skyrimo taisyklių pažeidimą, elektroninių ryšių tinklo gadinimą ar savavališką prisijungimą prie tinklo arba galinių įrenginių, trukdančių elektroninių ryšių tinklo darbui, savavališką prisijungimą arba elektroninių ryšių infrastruktūros įrengimo, naudojimo ir apsaugos sąlygų ir taisyklių pažeidimą, jeigu nuo jos paskyrimo praėję mažiau kaip vieni metai.

21. Saugos įgaliotinis privalo išmanyti elektroninės informacijos saugos užtikrinimo principus, tobulinti kvalifikaciją informacijos saugos srityje.

22. Saugos įgaliotinis atlieka šias funkcijas:

22.1. teikia Įmonės vadovui pasiūlymus dėl:

22.1.1. administratoriaus (administratorių) paskyrimo ir reikalavimų administratoriui (administratoriams) nustatymo;

22.1.2. Įmonės ITT saugos atitikties vertinimo atlikimo;

22.1.3. saugos dokumentų priėmimo, keitimo;

22.2. koordinuoja elektroninės informacijos saugos incidentų, įvykusių informacinėje sistemoje, tyrimą ir bendradarbiauja su kompetentingomis institucijomis, tiriančiomis elektroninių ryšių tinklų, informacijos saugos incidentus, neteisėtas veikas, susijusias su elektroninės informacijos saugos incidentais, išskyrus tuos atvejus, kai šią funkciją atlieka elektroninės informacijos saugos darbo grupės;

22.3. teikia administratoriui (administratoriams) ir informacinės sistemos naudotojams privalomus vykdyti nurodymus ir pavedimus, susijusius su saugos politikos įgyvendinimu;

22.4. organizuoja rizikos vertinimą;

22.5. atlieka kitas saugos nuostatuose, Reikalavimuose ir kituose teisės aktuose jam priskirtas funkcijas.

23. Saugos įgaliotinis negali atlikti administratoriaus funkcijų.

24. Saugos įgaliotinis organizuoja informacinės sistemos naudotojų periodinius mokymus informacijos saugos klausimais, informuoja juos apie elektroninės informacijos saugos problemas. Mokymo ir informavimo būdai pasirenkami atsižvelgiant į informacinės sistemos specifiką.

25. Administratorius atlieka funkcijas, susijusias su informacinės sistemos naudotojų teisių valdymu, informacinės sistemos sudedamosiomis dalimis (kompiuteriais, operacinėmis sistemomis, duomenų bazių valdymo sistemomis, taikomųjų programų sistemomis, ugniasienėmis, įsilaužimų aptikimo sistemomis, elektroninės informacijos perdavimu tinklais, bylų serveriais ir kitais), šių informacinės sistemos sudedamųjų dalių sąranka, informacinių sistemų pažeidžiamų vietų nustatymu, saugos reikalavimų atitikties nustatymu ir stebėsena, reagavimu į elektroninės informacijos saugos incidentus, taip pat privalo vykdyti visus saugos įgaliotinio nurodymus ir pavedimus, susijusius su informacinės sistemos saugos užtikrinimu, ir nuolat teikti saugos įgaliotiniui informaciją apie saugą užtikrinančių pagrindinių informacinės sistemos sudedamųjų dalių būklę.

26. Keisdamas informacinės sistemos sąranką, administratorius turi laikytis Įmonėje nustatytos informacinės sistemos pokyčių valdymo tvarkos, nustatytos elektroninės informacijos saugaus tvarkymo taisyklėse.

27. Administratorius privalo patikrinti informacinės sistemos sąranką ir informacinės sistemos būsenos rodiklius reguliariai, ne rečiau kaip kartą per metus ir (arba) po informacinės sistemos pokyčio.

28. Įmonėje, kurioje veikia daugiau kaip 2 informacinės sistemos ar informacinės sistemos, kurias sudaro ne mažiau kaip 2 posistemiai ar funkciškai savarankiškos sudedamosios dalys, galima sudaryti informacijos saugos darbo grupes, koordinuosiančias saugos politikos įgyvendinimą Įmonėje, elektroninės informacijos saugos priemonių ir metodų taikymą Įmonėje ir jos informacinėse sistemose, analizuosiančias ir koordinuosiančias Įmonės informacinėse sistemose įvykusių informacijos saugos incidentų tyrimą ir tvarkysiančias saugos dokumentus.

29. Saugos įgaliotinis ir administratorius gali būti paskiriami Įmonės informacinėms sistemoms, posistemiams, funkciškai savarankiškoms sudedamosioms dalims prižiūrėti ar tam tikroms saugos įgaliotinio ir administratoriaus funkcijoms atlikti, tačiau turi būti užtikrintas tinkamas saugos įgaliotinio ir administratoriaus funkcijų atlikimas. Jeigu vienas saugos įgaliotinis ir administratorius skiriamas prižiūrėti ne visas valdomas informacines sistemas, posistemius, funkciškai savarankiškas sudedamąsias dalis ar atlikti tik tam tikras saugos įgaliotinio ir administratoriaus funkcijas, turi būti aiškiai nurodyta, kokiai informacinei sistemai, posistemiui, funkciškai savarankiškoms sudedamosioms dalims prižiūrėti ar kurioms saugos įgaliotinio ir administratoriaus funkcijoms atlikti paskiriamas konkretus saugos įgaliotinis ir administratorius, taip pat vienam iš saugos įgaliotinių ir administratorių turi būti pavedama koordinuoti šių saugos įgaliotinių ir administratorių veiklą.

V SKYRIUS
INFORMACIJOS SAUGOS TECHNINIAI REIKALAVIMAI

30. ITT saugos atitiktis turi būti vertinama ne rečiau kaip kartą per metus. Ne rečiau kaip kartą per 3 metus ITT saugos atitiktis turi būti vertinama nepriklausomų, visuotinai pripažintų tarptautinių organizacijų sertifikuotų auditorių, vertinančių informacines sistemas.

31. Informacinėje sistemoje turi būti įrašomi ir elektroninės informacijos saugaus tvarkymo taisyklėse nustatytą laiką (ne trumpiau kaip 1 metus) saugomi duomenys apie informacinės sistemos tarnybinių stočių, informacinės sistemos taikomosios programinės įrangos įjungimą, išjungimą, sėkmingus ir nesėkmingus bandymus registruotis informacinės sistemos tarnybinėse stotyse, informacinės sistemos taikomojoje programinėje įrangoje, visus informacinės sistemos naudotojų

vykdomus veiksmus, kitus elektroninės informacijos saugai svarbius įvykius, taip pat nurodomas informacinės sistemos naudotojo identifikatorius ir elektroninės informacijos saugai svarbaus įvykio ar vykdyto veiksmo laikas; šie duomenys turi būti saugomi ne toje pačioje informacinėje sistemoje, kurioje jie įrašomi, taip pat šie duomenys turi būti analizuojami ne rečiau kaip kartą per savaitę.

32. Informacinės sistemos priežiūros funkcijos turi būti atliekamos naudojant atskirą tam skirtą informacinės sistemos administratoriaus paskyrą, kuria naudojantis negalima atlikti informacinės sistemos naudotojo funkcijos.

33. Informacinių sistemų naudotojams negali būti suteikiamos informacinės sistemos administratoriaus teisės.

34. Kiekvienas informacinės sistemos naudotojas informacinėje sistemoje turi būti unikaliai identifikuojamas (asmens kodas negali būti naudojamas kaip informacinės sistemos naudotojo identifikatorius).

35. Nuotolinis prisijungimas prie informacinės sistemos turi būti vykdomas pagal protokolą, skirtą duomenims šifruoti.

36. Informacinės sistemos naudotojas ar informacinės sistemos administratorius turi patvirtinti savo tapatybę slaptažodžiu arba kita autentiškumo patvirtinimo priemone.

37. Vidiniam informacinės sistemos naudotojui teisė dirbti su konkrečia elektronine informacija turi būti sustabdoma, kai vidinis informacinės sistemos naudotojas nesinaudoja informacine sistema ilgiau kaip 3 mėnesius, kai vidinis informacinės sistemos naudotojas nušalinamas nuo darbo (pareigų); pasibaigus tarnybos (darbo) santykiams, vidinio informacinės sistemos naudotojo teisė naudotis informacine sistema turi būti panaikinta nedelsiant.

38. Baigus darbą ar pasitraukiant iš darbo vietos informacinėje sistemoje turi būti imamasi priemonių, kad su elektronine informacija negalėtų susipažinti pašaliniai asmenys: atsijungiama nuo informacinės sistemos, įjungiama ekrano užsklanda su slaptažodžiu; dokumentai ar jų kopijos darbo vietoje turi būti padedami į pašaliniams asmenims neprieinamą vietą.

39. Informacinės sistemos naudotojui neatliekant jokių veiksmų informacinėje sistemoje, informacinės sistemos taikomoji programinė įranga turi užsirakinti tam, kad toliau naudotis informacine sistema būtų galima tik pakartotinai patvirtinus savo tapatybę; laikotarpis, per kurį informacinės sistemos naudotojui neatliekant jokių veiksmų informacinės sistemos taikomoji programinė įranga užsirakina, nustatomas informacinės sistemos valdytojo tvirtinamose elektroninės informacijos saugaus tvarkymo taisyklėse; laikotarpis, per kurį informacinės sistemos naudotojui neatliekant jokių veiksmų informacinės sistemos taikomoji programinė įranga turi užsirakinti, negali būti ilgesnis nei 15 minučių.

40. Įmonės nustatytas maksimalus informacinės sistemos ar jos dalies neveikimo laikotarpis, per kurį informacinės sistemos tvarkytojas dar gali atlikti funkcijas, kurioms atlikti buvo sukurta informacinė sistema, negali būti ilgesnis nei 8 valandos.

41. Informacinės sistemos techninės ir programinės įrangos ir patalpų reikalavimai:

41.1. pagrindinė informacinės sistemos kompiuterinė įranga turi turėti įtampos filtrą ir rezervinį maitinimo šaltinį, užtikrinantį informacinės sistemos pagrindinės kompiuterinės įrangos veikimą;

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

41.3. informacinės sistemos tarnybinėse stotyse ir vidinių informacinės sistemos naudotojų kompiuteriuose turi būti naudojamos centralizuotai valdomos ir atnaujinamos kenksmingosios programinės įrangos aptikimo, stebėjimo realiu laiku priemonės; šios priemonės automatiškai turi informuoti informacinės sistemos administratorių, kuriems informacinės sistemos posistemiams, funkciškai savarankiškoms sudedamosioms dalims yra pradelstas kenksmingosios programinės įrangos aptikimo priemonių atsinaujinimo laikas; informacinės sistemos sudedamosios dalys be kenksmingo programinės įrangos aptikimo priemonių gali būti eksploatuojamos, jeigu rizikos

vertinimo metu yra patvirtinama, kad šioms informacinės sistemos sudedamosioms dalims keliama rizika yra priimtina;

41.4. turi būti operatyviai testuojami ir diegiami informacinės sistemos tarnybinių stočių ir vidinių informacinės sistemos naudotojų darbo vietų kompiuterinės įrangos operacinės sistemos ir kitos naudojamos programinės įrangos gamintojų rekomenduojami atnaujinimai; informacinės sistemos administratorius reguliariai, ne rečiau kaip kartą per savaitę, turi įvertinti informaciją apie informacinės sistemos posistemiuose, funkciškai savarankiškose sudedamosiose dalyse, vidinių informacinės sistemos naudotojų darbo vietų kompiuterinėje įrangoje neįdiegtus rekomenduojamus gamintojų atnaujinimus ir susijusius saugos pažeidžiamumo svarbos lygius;

41.5. informacinės sistemos tarnybinėse stotyse turi būti naudojama tik legali programinė įranga;

41.6. vidinių informacinės sistemos naudotojų kompiuterinėje įrangoje turi būti naudojama tik legali ir darbo funkcijoms atlikti reikalinga programinė įranga; informacinės sistemos saugos įgaliotinis turi parengti, su Įmonės vadovu suderinti ir ne rečiau kaip kartą per metus peržiūrėti ir prireikus atnaujinti leistinos programinės įrangos sąrašą;

41.7. informacinės sistemos techninė ir programinė įranga turi būti prižiūrima laikantis gamintojo rekomendacijų;

41.8. prižiūrėti informacinės sistemos techninę ir programinę įrangą ir šalinti jos gedimus turi kvalifikuoti specialistai;

41.9. informacinės sistemos tarnybinių stočių patalpos turi būti apsaugotos nuo neteisėto asmenų patekimo į jas;

41.10. visose patalpose, kuriose yra vidinių informacinės sistemos naudotojų ir informacinės sistemos techninė įranga, turi būti įrengti gaisro ir įsilaužimo jutikliai, prijungti prie pastato signalizacijos ir (arba) apsaugos tarnybos stebėjimo pulto;

41.11. per metus turi būti užtikrintas informacinės sistemos prieinamumas visą parą ne mažiau kaip 99 proc. laiko;

41.12. Įmonės saugos nuostatuose nustatyta tvarka turi būti daromos atsarginės elektroninės informacijos kopijos (toliau – kopijos), kurios turi būti saugomos kitose patalpose, nei yra įrenginys, kurio elektroninė informacija buvo nukopijuota, arba kitame pastate;

41.13. elektroninė informacija kopijose turi būti užšifruota (šifravimo raktai turi būti saugomi atskirai nuo kopijų) arba turi būti imtasi kitų priemonių, neleidžiančių neteisėtai atkurti elektroninės informacijos, panaudojus kopijas;

41.14. atsarginės laikmenos su informacinės sistemos programinės įrangos kopijomis turi būti laikomos kitose patalpose arba kitame pastate, nei yra informacinės sistemos tarnybinės stotys;

41.15. informacinės sistemos elektroninės informacijos perdavimo tinklas turi būti atskirtas nuo viešųjų ryšių tinklų naudojant ugniasienę; ugniasienės įvykių žurnalai (angl. *Logs*) turi būti reguliariai analizuojami, o ugniasienės saugumo taisyklės periodiškai peržiūrimos ir atnaujinamos;

41.16. informacinės sistemos programinė įranga turi turėti apsaugą nuo pagrindinių per tinklą vykdomų atakų: SQL įskverbties (angl. *SQL injection*), XSS (angl. *Cross-site scripting*), atkirtimo nuo paslaugos (angl. *DOS*), dedikuoto atkirtimo nuo paslaugos (angl. *DDOS*) ir kitų; pagrindinių per tinklą vykdomų atakų sąrašas skelbiamas Atvirųjų interneto taikomųjų programų saugumo projekto (angl. *The Open Web Application Security Project*. OWASP) interneto svetainėje www.owasp.org.

42. Informacinės sistemos tinklo perimetro apsaugai turi būti naudojami filtrai, apsaugantys elektroniniame pašte ir viešajame ryšių tinkle naršančių informacinės sistemos naudotojų kompiuterinę įrangą nuo kenksmingo kodo.

43. Prisijungimo prie visų informacinių sistemų slaptažodžių reikalavimai:

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

43.2. slaptažodžiams sudaryti neturi būti naudojama asmeninio pobūdžio informacija;

43.3. draudžiama slaptažodžius atskleisti tretiesiems asmenims;

43.4. informacinės sistemos dalys, autentifikuojančios nutolusį prisijungimą, neturi leisti automatiškai išsaugoti slaptažodžių;

43.5. Įmonės informacinės sistemos naudotojų administravimo taisyklėse turi būti nustatytas ne didesnis nei 5 kartai didžiausias leistinas nesėkmingų mėginimų prisijungti, įvedant slaptažodį, skaičius, kurį viršijus informacinė sistema turi užsirakinti ir neleisti informacinės sistemos naudotojui identifikuotis Įmonės informacinės sistemos naudotojų administravimo taisyklėse nustatytą laiko tarpą, kuris negali būti trumpesnis nei 15 minučių;

43.6. slaptažodžiai negali būti saugomi ar perduodami atviru tekstu ar užšifruojami nepatikimais algoritmais; saugos įgaliotinio sprendimu tik laikinas slaptažodis gali būti perduodamas atviru tekstu, tačiau atskirai nuo prisijungimo vardo, jei:

43.6.1. informacinės sistemos naudotojas neturi galimybių iššifruoti gauto užšifruoto slaptažodžio;

43.6.2. nėra techninių galimybių informacinės sistemos naudotojui perduoti slaptažodžio šifruotu kanalu ar saugiu elektroninių ryšių tinklu;

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

43.8. slaptažodį turi sudaryti ne mažiau kaip 8 simboliai;

43.9. keičiant slaptažodį informacinė sistema neturi leisti sudaryti slaptažodžio iš buvusių 6 paskutinių slaptažodžių;

43.10. per pirmąjį prisijungimą prie informacinės sistemos iš informacinės sistemos naudotojo turi būti reikalaujama, kad jis pakeistų slaptažodį;

43.11. papildomi informacinės sistemos administratoriaus slaptažodžių reikalavimai:

43.11.1. slaptažodis turi būti keičiamas ne rečiau kaip kas 2 mėnesius;

43.11.2. slaptažodį turi sudaryti ne mažiau kaip 12 simbolių;

43.11.3. keičiant slaptažodį informacinės sistemos taikomoji programinė įranga neturi leisti sudaryti slaptažodžio iš buvusių 3 paskutinių slaptažodžių.

44. Informacinė sistema turi perspėti informacinės sistemos administratorių, kai pagrindinėje informacinės sistemos kompiuterinėje įrangoje iki nustatytos pavojingos ribos sumažėja laisva kompiuterio atmintis ar vieta diske, ilgą laiką stipriai apkraunamas centrinis procesorius ar kompiuterių tinklo sąsaja.

45. Viešaisiais ryšių tinklais perduodamos informacinės sistemos elektroninės informacijos konfidencialumas turi būti užtikrintas, naudojant šifravimą, virtualų privatų tinklą (angl. *virtual private network*), skirtines linijas, saugų elektroninių ryšių tinklą ar kitas priemones.

46. Informacinė sistema turi turėti įvestos elektroninės informacijos tikslumo, užbaigtumo ir patikimumo tikrinimo priemones.

47. Patekimas į informacinės sistemos tarnybinių stočių patalpas ir patalpas, kuriose saugomos atsarginės kopijos, turi būti kontroliuojamas Įmonės elektroninės informacijos saugaus tvarkymo taisyklėse nustatyta tvarka.

48. Įmonė turi numatyti atsargines patalpas, į kurias galėtų laikinai perkelti informacinės sistemos įrangą, jei nebūtų galimybės tęsti veiklą pagrindinėse patalpose; planas turi užtikrinti informacinės sistemos veiklos atnaujinimą atsarginėse patalpose per ne ilgesnį nei Reikalavimų 40 punkte nustatytą laikotarpį. Atsarginės patalpos turi tenkinti pagrindinėms patalpoms keliamus reikalavimus arba plane turi būti nustatyta, kaip per minimalų laikotarpį pasiekti šių reikalavimų atitiktį.

49. Atsarginės laikmenos su programinės įrangos kopijomis turi būti laikomos nedegioje spintoje, kitose patalpose arba kitame pastate, nei yra informacinės sistemos tarnybinės stotys.

50. Programinę įrangą turi diegti tik informacinės sistemos valdytojo ar tvarkytojo vadovo įgalioti asmenys.

51. Programinė įranga turi būti testuojama naudojant atskirą testuoti skirtą aplinką, kurioje esantys asmens duomenys turi būti naudojami vadovaujantis Bendrųjų reikalavimų organizacinėms ir techninėms duomenų saugumo priemonių, patvirtintų Valstybinės duomenų apsaugos inspekcijos

direktoriaus 2008 m. lapkričio 12 d. įsakymu Nr. 1T-71(1.12) „Dėl Bendrųjų reikalavimų organizacinėms ir techninėms duomenų saugumo priemonėms patvirtinimo“, 10.10 papunkčio reikalavimais.

52. Vidinių informacinės sistemos naudotojų darbo vietose gali būti naudojamos tik tarnybinėms reikmėms skirtos išorinės duomenų laikmenos (pavyzdžiui, USB raktai, CD / DVD ir kita); šios laikmenos negali būti naudojamos veiklai, nesusijusiai su teisėtu informacinės sistemos tvarkymu.

53. Svarbiausia kompiuterinė įranga ir duomenų perdavimo tinklo mazgai turi turėti rezervinį maitinimo šaltinį, užtikrinsiantį šios įrangos veikimą ne trumpiau kaip 30 minučių.

54. Svarbiausia kompiuterinė įranga, duomenų perdavimo tinklo mazgai ir ryšio linijos turi būti dubliuoti, o jų techninė būklė nuolat stebima.

55. Svarbiausios kompiuterinės įrangos gedimai turi būti registruojami, taip pat turi būti paskirtas asmuo, atsakingas už gedimų registravimą.

56. Patekimas prie vidinių informacinės sistemos naudotojų darbo vietų turi būti kontroliuojamas.

57. Pagrindinėse informacinės sistemos tarnybinėse stotyse turi būti naudojamos vykdomo kodo kontrolės priemonės, automatiškai apribojančios ar informuojančios apie neautorizuoto programinio kodo vykdymą.

58. Pagrindinėse informacinės sistemos tarnybinėse stotyse turi būti įjungtos ugniasienės, sukonfigūruotos praleisti tik su informacinės sistemos funkcionalumu ir administravimu susijusį duomenų srautą; ugniasienių konfigūracijų dokumentacija turi būti saugoma kartu su informacinės sistemos dokumentacija.

59. Informacinės sistemos tinkle turi būti įdiegtos ir veikti automatinės įsilaužimo aptikimo sistemos.

60. Įmonė turi įgyvendinti Lietuvos standarte LST ISO/IEC 27002:2009 nurodytas saugos priemones, išskyrus priemones, netaikytinas dėl Įmonės veiklos, informacinės sistemos ar naudojamos informacinėje sistemoje techninės įrangos pobūdžio, ir Lietuvos standarte LST ISO/IEC 27001:2006 nurodytus informacijos saugos valdymo sistemos reikalavimus.

VI SKYRIUS
INFORMACINĖS SAUGOS INCIDENTŲ VALDYMAS

61. Informacinės sistemos naudotojai, pastebėję saugos dokumentuose nustatytų reikalavimų pažeidimų, nusikalstamos veikos požymių, neveikiančias arba netinkamai veikiančias saugos užtikrinimo priemones, privalo nedelsdami pranešti administratoriui, saugos įgaliotiniui.

62. Jeigu saugos įgaliotinis nebuvo informuotas apie Reikalavimų 61 punkte nurodytus pažeidimus, administratorius arba informacinių technologijų pagalbos tarnyba informuoja saugos įgaliotinį apie šiuos pažeidimus. Įtaręs neteisėtą veiką, pažeidžiančią ar neišvengiamai pažeisiančią informacinės sistemos saugą, saugos įgaliotinis turi pranešti Įmonės vadovui ir kompetentingoms institucijoms, tiriančioms elektroninių ryšių tinklų, informacijos saugos incidentus, neteisėtas veikas, susijusias su elektroninės informacijos saugos incidentais.

63. Elektroninės informacijos saugos incidentų, įvykusių informacinėje sistemoje, tyrimo tvarka nustatoma plane.

VII SKYRIUS
RIZIKOS VERTINIMAS

64. Saugos įgaliotinis, atsižvelgdamas į Lietuvos ir tarptautinius grupės „Informacijos technologija. Saugumo technika“ standartus, kasmet organizuoja visų informacinių sistemų rizikos įvertinimą. Prireikus saugos įgaliotinis gali organizuoti neeilinį informacinių sistemų rizikos įvertinimą. Įmonės vadovo rašytiniu pavedimu informacinių sistemų rizikos įvertinimą gali atlikti pats saugos įgaliotinis. Organizuojant informacinių sistemų rizikos įvertinimą rekomenduojama

naudotis Vidaus reikalų ministerijos išleista metodine priemone „Rizikos analizės vadovas“, paskelbta Vidaus reikalų ministerijos interneto svetainėje (http://www.vrm.lt/Rizikos_analize.pdf).

65. Informacinių sistemų rizikos įvertinimo rezultatai išdėstomi rizikos įvertinimo ataskaitoje, kuri pateikiama Įmonės vadovui. Rizikos įvertinimo ataskaita rengiama įvertinant rizikos veiksnius, galinčius turėti įtakos elektroninės informacijos saugai, jų galimą žalą, pasireiškimo tikimybę ir pobūdį, galimus rizikos valdymo būdus, rizikos priimtinumo kriterijus. Svarbiausieji rizikos veiksniai yra šie:

65.1. subjektyvūs netyčiniai (elektroninės informacijos tvarkymo klaidos ir apsirikimai, elektroninės informacijos ištrynimas, klaidingas elektroninės informacijos teikimas, fiziniai elektroninės informacijos technologijų sutrikimai, elektroninės informacijos perdavimo tinklais sutrikimai, programinės įrangos klaidos, neteisingas veikimas ir kita);

65.2. subjektyvūs tyčiniai (nesankcionuotas naudojimasis informacine sistema elektroninei informacijai gauti, elektroninės informacijos pakeitimas ar sunaikinimas, informacinių technologijų duomenų perdavimo tinklais sutrikdymai, saugumo pažeidimai, vagystės ir kita);

65.3. atsiradę dėl nenugalimos jėgos (*force majeure*).

VIII SKYRIUS
INFORMACINĖS SISTEMOS POKYČIŲ VALDYMAS

66. Įmonėje turėtų būti planuojamas pokyčių valdymas. Pokyčių planas turi apimti pokyčių identifikavimą, suskirstymą į kategorijas pagal pokyčio tipą (administracinis, organizacinis ar techninis), įtakos vertinimą ir pokyčių prioritetų nustatymo procesus. Su tuo susijusios nuostatos nustatomos Įmonės elektroninės informacijos saugaus tvarkymo taisyklėse.

67. Visi pokyčiai, galintys sutrikdyti ar sustabdyti informacinės sistemos darbą, turi būti suderinti ir vykdomi tik gavus Įmonės vadovo raštišką pritarimą. Pokyčius turi teisę inicijuoti saugos įgaliotinis ar administratorius, o įgyvendinti – administratorius.

68. Informacinės sistemos sąrankos aprašai turi būti nuolat atnaujinami ir rodyti esamą informacinės sistemos sąrankos būklę.

69. Pokyčiai, galintys daryti neigiamą įtaką elektroninės informacijos konfidencialumui, vientisumui ar prieinamumui, turi būti patikrinti bandomojoje aplinkoje, kurioje nėra konfidencialių ir asmens duomenų ir kuri atskirta nuo eksploatuojamos informacinės sistemos.

IX SKYRIUS
ITT SAUGOS ATITIKTIES VERTINIMAS

70. ITT saugos atitiktis vertinama vadovaujantis Informacinių technologijų saugos atitikties metodika, patvirtinta vidaus reikalų ministro įsakymu.

71. Atlikus ITT saugos atitikties vertinimą, rengiama ITT saugos atitikties vertinimo ataskaita, kuri pateikiama Įmonės vadovui. Įmonės vadovas tvirtina pastebėtų trūkumų šalinimo planą, paskiria atsakingus vykdytojus ir nustato įgyvendinimo terminą.

X SKYRIUS
INFORMACINĖS SISTEMOS NAUDOTOJŲ ATSAKOMYBĖ

72. Tvarkyti informacinės sistemos elektroninę informaciją gali tik informacinės sistemos naudotojai, susipažinę su saugos dokumentais ir sutikę laikytis jų reikalavimų.

73. Saugos įgaliotinis imasi priemonių, kad informacinės sistemos naudotojai būtų pasirašytinai supažindinti su saugos dokumentais ir atsakomybe už jų reikalavimų nesilaikymą.

74. Informacinės sistemos naudotojai, pažeidę Reikalavimų ir kitų saugų elektroninės informacijos tvarkymą reglamentuojančių teisės aktų nuostatas, atsako įstatymų nustatyta tvarka.

75. Informacinės sistemos naudotojai privalo saugoti slaptą informaciją. Įsipareigojimas saugoti slaptą informaciją galioja ir nutraukus su elektroninės informacijos tvarkymu susijusią veiklą.

XI SKYRIUS
BAIGIAMOSIOS NUOSTATOS

76. Įmonės visų lygių vadovai, užtikrindami Reikalavimų įgyvendinimą, privalo periodiškai, ne rečiau kaip kartą per metus, vertinti Reikalavimų vykdymą ir šalinti trūkumus jiems pavaldžiuose padaliniuose.

_____

SUDERINTA
Lietuvos Respublikos
vidaus reikalų ministerijos
2013-12-20 raštu Nr. 1D-11374(3)

SUDERINTA
Lietuvos Respublikos
valstybės saugumo departamento
2013-10-28 raštu Nr. (63)-18-4072-2763

Pakeitimai:

1.
Lietuvos Respublikos ūkio ministerija, Įsakymas
Nr. 4-79, 2014-02-05, paskelbta TAR 2014-02-06, i. k. 2014-01211
Dėl Lietuvos Respublikos ūkio ministro 2004 m. rugsėjo 22 d. įsakymo Nr. 4-349 „Dėl strateginę reikšmę nacionaliniam saugumui turinčių, Ūkio ministerijos valdymo sričiai priskirtų įmonių ir įrenginių bei kitų nacionaliniam saugumui užtikrinti svarbių įmonių informacinės saugos reikalavimų patvirtinimo“ pakeitimo