PATVIRTINTA
SĮ „Vilniaus atliekų sistemos administratorius“ valdybos 2025 m. birželio 27 d. sprendimu Nr. **LKG-2025-15**

SĮ „VILNIAUS ATLIEKŲ SISTEMOS ADMINISTRATORIUS“ KIBERNETINIO SAUGUMO POLITIKA

TURINYS

I. VERSIJAVIMAS

Versija	Rengimo data	Rengėjas	Aprašymas
1.0	2022-01-13	IT skyriaus vadovas	Naujas dokumentas “Informacijos saugumo politika”
2.0	2025-06-20	IT skyriaus vadovas ir Kibernetinio saugumo vadovas	Naujas dokumentas “Kibernetinio saugumo politika”. Peržiūrėti, atnaujinti ir įtraukti nauji techninių ir organizacinių priemonių reikalavimai visuose skyriuose jog atitiktų atnaujintus kibernetinio saugumo įstatymo reikalavimus. Nauji skyriai: • Versijavimas • Sąvokos, sutrumpinimai ir apibrėžimai • Atsakomybės • Mokymai • Nuotolinio darbo reikalavimai • Keitimų valdymas • Saugumo operacijos centras (SOC) • Santykiai su išorinėmis šalimis • Kelių veiksnių tapatumo nustatymo sprendimai • Susiję dokumentai Naujos tvarkos/reikalavimai susiję su kibernetinio saugumo politika: • Informacijos klasifikavimo reikalavimai • Paslaugų teikėjų ir tiekimo grandinės valdymo reikalavimai • Kriptografijos ir šifravimo naudojimo tvarka • Pažeidžiamumų valdymo tvarka • Kelių veiksnių tapatumo nustatymo sprendimų, saugių balso, vaizdo ir teksto ryšių bei saugių avarinių sistemų subjekto viduje naudojimo tvarka • Kibernetinio saugumo reikalavimų veiksmingumo vertinimo tvarka • Tinklų ir informacinių sistemų fizinės prieigos reikalavimai

			• Saugumo operacijų centro valdymo tvarka Pakeistas skyriaus pavadinimas: • iš "Ryšių saugumas" į „Tinklo valdymo priemonės" Nauja rolė: • Kibernetinio saugumo vadovas • Saugumo operacijų centras (SOC) • Duomenų apsaugos pareigūnas (DAP)

II. BENDROSIOS NUOSTATOS

1. Kibernetinio saugumo politika (toliau – Politika) nustato SĮ „Vilniaus atliekų sistemos administratorius" (toliau – Įmonė) informacijos saugumo organizavimo principus ir informacijos saugumo reikalavimus tinkamai Informacinių išteklių saugai nuo išorės bei vidaus grėsmių.

III. SĄVOKOS, SUTRUMPINIMAI IR APIBRĖŽIMAI

2. Politikoje naudojamos sąvokos, sutrumpinimai ir apibrėžimai:

Sąvoka, sutrumpinimai	Apibrėžimas
Politika	SĮ „Vilniaus atliekų sistemos administratorius" Kibernetinio saugumo politika.
DAP	Duomenų apsaugos pareigūnas. VASA vadovo paskirtas darbuotojas ar paslaugų teikėjas, administruojantis asmens duomenų apsaugos klausimus.
Kibernetinio saugumo vadovas	VASA vadovo paskirtas darbuotojas ar paslaugų teikėjas, administruojantis kibernetinio saugumo klausimus.
KSIS	NKSC Kibernetinio saugumo informacinė sistema.
JIRA	Projektų valdymo sistema.
NKSC	Nacionalinis kibernetinio saugumo centras prie Krašto apsaugos ministerijos.
RIS	Ryšiai ir informacinės sistemos.
VASA	Savivaldybės įmonė „Vilniaus atliekų sistemos administratorius" (VASA).
VDAI	Valstybinė duomenų apsaugos inspekcija.

VT komanda	Veiklos tęstinumo valdymo komanda.
VTVP	Veiklos tęstinumo valdymo planas.
Sistemų administratorius	Įmonės darbuotojas, kuris prižiūri, konfigūruoja Įmonės informacinius išteklius.
Saugumo operacijų centras (SOC)	Įmonės komanda arba centralizuota funkcija, atsakinga už organizacijos kibernetinio saugumo būsenos gerinimą, grėsmių prevenciją, aptikimą bei reagavimą į jas.
Konfidencialumas	Informacijos savybė, reiškianti, kad su ja gali susipažinti tik tam įgalioti asmenys.
Vientisumas	Informacijos savybė, reiškianti, kad informacija nebuvo atsitiktiniu ar neteisėtu būdu pakeista ar sunaikinta.
Prieinamumas	Informacijos savybė, reiškianti, kad informacija gali būti tvarkoma reikiamu metu.
Informacijos sauga	Informacijos konfidencialumo, prieinamumo ir vientisumo užtikrinimas.
Informaciniai ištekliai	Įmonės Informacija, tvarkomos Informacinės sistemos, informacinių technologijų funkcionavimui reikalingos paslaugos, darbuotojų žinios.
Informacija	bet kokia Įmonės ar jai pateikta informacija (žinios apie faktus, įvykius, daiktus, procesus, idėjas, sąvokas ir kitus objektus, kurios kuriame nors kontekste turi kokią nors prasmę), nepriklausomai nuo to, kokioje laikmenoje ji užfiksuota arba kokiu būdu pateikiama ar perduodama.
Informacinės sistemos	Apima visus Įmonės serverius ir vartotojo įrenginius, kaip kompiuteriai, telefonai, planšetės, išorinės laikmenos, tinklo infrastruktūra, sisteminė (operacinės sistemos, archyvavimo programinė įranga, kt.) ir taikomoji programinė įranga (biuro programų paketai, specializuota programinė įranga, kt.), duomenys, kiti kompiuteriniai komponentai ar sistemos, kurie priklauso Įmonei ar yra naudojami Įmonėms reikmėms. Tokioms informacinėms sistemoms priklauso visos vidinės ir išorinės paslaugos, kaip Interneto prieiga, elektroninis paštas, komunikacijos priemonės.
ISVS	Informacijos saugos valdymo sistema – rizikų valdymu pagrįsta Įmonės vadybos sistemos dalis, kuria siekiama sukurti, įgyvendinti, valdyti, stebėti, vertinti, prižiūrėti ir gerinti Informacijos saugą.
Išorinės šalys	paslaugų teikėjai, partneriai, klientai, kiti asmenys ir organizacijos, turintys ar galintys turėti prieigą prie Įmonės informacinių išteklių.

Naudotojas	Įmonės ar Išorinės šalies darbuotojas, kuriam suteikta teisė naudotis Įmonės informaciniais ištekliais.
ITT	informacinės technologijos ir telekomunikacijos.
Kibernetinis incidentas	įvykis, dėl kurio kyla pavojus saugomų, perduodamų arba tvarkomų duomenų arba paslaugų, teikiamų arba prieinamų per tinklų ir informacines sistemas, prieinamumui, autentiškumui, vientisumui arba konfidencialumui.
Kelių veiksnių autentifikavimas (MFA)	autentifikavimo metodas, reikalaujantis dviejų ar daugiau nepriklausomų veiksnių patvirtinimo.
Nuolatinis tapatumo tikrinimas	vartotojo identiteto patvirtinimas nuolat naudojant biometrinius duomenis ar elgsenos analizę, kontekstinę informaciją ir kt.
Avarinės sistemos	ryšių kanalai, naudojami ekstremalių situacijų metu, nepriklausomi nuo pagrindinės infrastruktūros.
Rizika	potencialios grėsmės poveikio tikimybė ir jos galimas poveikis

IV. INFORMACIJOS SAUGOS ORGANIZAVIMAS

3. Pagrindinis Įmonės Politikos tikslas – Įmonės valdomos Informacijos konfidencialumo, vientisumo ir prieinamumo užtikrinimas, bei kylančių rizikų sumažinimas iki priimtino lygio. Įmonės informacijos saugos valdymas grindžiamas rizikų vertinimu, t. y. naudojamos informacijos saugos priemonės atitinka informacijos svarbą ir jai kylančias rizikas.
4. Įmonės vadovybė Informacijos saugos valdymą laiko neatsiejama Įmonės veiklos dalimi ir įsipareigoja skirti visą reikalingą dėmesį ir išteklius užtikrinant Informacijos saugos tikslo įgyvendinimą.
5. Įmonės vadovybė atsakinga už Informacijos saugos tikslo, suderinto su Įmonės veiklos strategija ir tikslais, nustatymą ir komunikavimą.
6. Įmonės vadovybė užtikrina Informacijos saugos valdymo sistemos nuolatinį tobulinimą, periodišką peržiūrėjimą ir gerinimą. Užtikrinant informacijos saugą Įmonėje, vadovaujamasi pripažintais Lietuvos ir tarptautiniais standartais (pvz., ISO/IEC 27000) ir metodikomis.
7. Įmonė privalo identifikuoti ir dokumentuoti visus Įmonei taikomus informacijos saugos reikalavimus, įskaitant:
   7.1. Teisės aktų reikalavimus:
      7.1.1. 2014 d. gruodžio 11 d. Lietuvos Respublikos kibernetinio saugumo įstatymu Nr. XII-1428 ir vėlesnius pakeitimus;
      7.1.2. Nacionaliniu kibernetinių incidentų valdymo planu, patvirtintu Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo dėl Nacionalinės kibernetinio saugumo strategijos patvirtinimo“;
      7.1.3. 1996 m. birželio 11 d. Lietuvos Respublikos asmens duomenų apsaugos įstatymu

Nr. I-1374;

7.1.4. Lietuvos Respublikos standartu LST EN ISO/IEC 27001:2022 „Informacinės technologijos. Saugumo metodai. Informacijos saugumo valdymo sistemos. Reikalavimai“;

7.1.5. Lietuvos Respublikos standartu LST EN ISO/IEC 27002:2022 „Informacinės technologijos. Saugumo metodai. Informacijos saugumo kontrolės priemonių praktikos nuostatai“;

7.1.6. Lietuvos Respublikos standartu LST EN ISO/IEC 27005:2022 „Informacinės technologijos. Saugumo metodai. „Informacijos saugumo rizikos valdymo gairės“;

7.1.7. Informacijos, reikalingos kibernetiniams incidentams, galimai turintiems nusikalstamos veikos požymių, užkardyti ir tirti, pateikimo, policijos nurodymų vykdymo bei kibernetinių incidentų tyrimo tvarkos aprašu, patvirtintu Lietuvos policijos generalinio komisaro 2015 m. vasario 2 d. įsakymu 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“;

7.2. Įmonės teisės aktų reikalavimus;

7.3. Veiklą prižiūrinčių įmonių reikalavimus;

7.4. Sutartinių įsipareigojimų reikalavimus.

8. Už Politikos ir ISVS įgyvendinimą atsakingas Įmonės vadovas. Informacijos saugos vertinimo, planavimo, įgyvendinimo ir kontrolės funkcijos gali būti deleguotos Kibernetinio saugumo vadovui ir/ar IT skyriaus vadovui.
9. Informacijos sauga yra kiekvieno darbuotojo atsakomybė. Darbuotojai privalo informuoti Įmonės vadovybę ir/ar jos paskirtą atsakingą asmenį – Kibernetinio saugumo vadovą, apie pastebėtus Informacijos/kibernetinės saugos incidentus.

V. INFORMACIJOS SAUGOS ORGANIZACINIAI PRINCIPAI

10. **Teisinis informacijos saugos organizavimo pagrįstumas**. Įmonės ISVS organizuojama vadovaujantis Įmonei nustatytais informacijos saugos reikalavimais.
11. **Tinkamos kompetencijos, įgaliojimų ir resursų suteikimas**. Politiką ir jos pagrindu sukurtą Įmonės ISVS įgyvendinantis asmuo (asmenys) turi turėti reikiamas kompetencijas ir jam (jiems) suteikiami reikalingi įgaliojimai bei resursai.
12. **Įmonės Informacinių išteklių žinojimas ir klasifikavimas**. Visi Įmonės Informaciniai ištekliai turi būti žinomi, jų valdymui ir prieigos suteikimui prie jų turi būti priskirti atsakingi valdytojai.
13. **Informacijos saugumo rizikų vertinimas**. Įmonės ISVS projektuojama ir įgyvendinama atsižvelgiant į Informacijos saugumo rizikų vertinimo Įmonės Informaciniams ištekliams rezultatus. Vertinant rizikas atsižvelgiama į Įmonės veiklos ir valdomos informacijos svarbą, galimas grėsmes ir pažeidžiamumus. Informacijos saugumo rizikų valdymas turi būti periodinis ir integruotas į esamą Įmonės rizikos valdymo procesą.
14. **Informacijos saugos valdymo priemonių proporcingumas**. Parinktos Informacijos saugos valdymo priemonės turi sumažinti nustatytą riziką, padidinti Informacijos saugumo lygį, užtikrinti veiklos tęstinumą, užtikrinti nuolatinę informacinių išteklių apsaugą bei būti orientuotos į prevenciją ir galimos žalos sumažinimą. Šių priemonių įgyvendinimo ir palaikymo kaštai negali būti didesni nei galimos pasekmės, jeigu tos priemonės nebūtų taikomos. Parinktų valdymo priemonių efektyvumas turi būti reguliariai stebimas.
15. **Gerųjų praktikų panaudojimas**. ISVS įgyvendinama taikant tarptautinius standartus ISO/IEC

27001:2022 „Informacijos technologija. Saugumo metodai. Informacijos saugumo valdymo sistemos. Reikalavimai“ bei ISO/IEC 27002:2022 „Informacinės technologijos. Saugumo metodai. Informacijos saugumo kontrolės priemonių praktikos kodeksas/nuostatai“ tokia apimtimi, kiek jų taikymas neprieštarauja LR įstatymams ir susijusiems poįstatyminiams teisės aktams.

16. **Sąmoningumo Informacijos saugos klausimais didinimas**. Įmonės darbuotojai turi turėti pakankamas informacijos saugos žinias ir šios žinios turi būti periodiškai atnaujinamos. Kiekvienas darbuotojas privalo elgtis su informacija taip, kad nesukeltų informacijos saugumo grėsmių.
17. **Atsakomybė už informacijos saugumo pažeidimus**. Už Politikos ir ją įgyvendinančių teisės aktų pažeidimus atsakoma LR įstatymuose ir Įmonės vidiniuose teisės aktuose nustatyta tvarka.

VI. ATSAKOMYBĖS

18. Už Politikos valdymą, priežiūrą ir organizavimą atsakingi asmenys:

18.1. Įmonės vadovas;
18.2. IT skyriaus vadovas;
18.3. Kibernetinio saugumo vadovas;
18.4. Duomenų apsaugos pareigūnas (DAP);
18.5. Sistemų administratorius;
18.6. Darbuotojai.

19. Įmonės vadovo atsakomybė informacijos saugos srityje:

19.1. paskirsto atsakomybes už Informacijos ir asmens duomenų saugą;
19.2. tvirtina informacijos saugumą reglamentuojančius dokumentus;
19.3. paskiria Kibernetinio saugumo vadovą;
19.4. užtikrina, kad NKSC būtų informuotas apie paskirtus už kibernetinį saugumą atsakingus asmenis per KSIS ir būtų pateikta KSIS nuostatuose nurodyto turinio kontaktinė informacija;
19.5. komunikuoja darbuotojams informacijos saugos reikalavimų laikymosi svarbą;
19.6. nustato kibernetinės higienos praktikos organizavimo ir kibernetinio saugumo mokymų organizavimo ir vykdymo tvarką;
19.7. nustato priimtiną kibernetinės saugos lygį Įmonėje;
19.8. nustato tinklų ir informacinių sistemų rizikos vertinimo ir valdymo tvarką;
19.9. tvirtina tinklų ir informacinių sistemų fizinės prieigos reikalavimus.

20. IT skyriaus vadovas:

20.1. Įgyvendina ir kontroliuoja Politikos įgyvendinimą;
20.2. nagrinėja ir svarsto klausimus, susijusius su Informacinių išteklių sauga ir jų naudojimu;
20.3. dalyvauja nagrinėjant klausimus susijusius su Kibernetiniais saugos incidentais;
20.4. užtikrina, kad Įmonė vadovaujasi informacijos saugą reglamentuojančiais teisės aktais, vertina atitiktį jų reikalavimams;
20.5. dalyvauja atliekant veiklos tęstinumo valdymo plano bandymus;
20.6. teikia Sistemų administratoriui nurodymus susijusius su Politikos įgyvendinimu;
20.7. bendradarbiauja su DAP asmens domenų apsaugos klausimais;
20.8. kontroliuoja IT ūkį aptarnaujančius paslaugų teikėjus;
20.9. nustato priimtino turto panaudojimo tvarką.
20.10. teikia pasiūlymus Įmonės vadovui dėl Sistemų administratoriaus skyrimo.

21. Kibernetinio saugumo vadovas:

21.1. vertina Politikos įgyvendinimą;

21.2. nagrinėja ir svarsto klausimus, susijusius su Informacinių išteklių sauga ir jų naudojimu;

21.3. nagrinėja, analizuoja ir kontroliuoja klausimus susijusius su Kibernetiniais saugos incidentais, bendradarbiauja su kompetentingomis institucijomis;

21.4. organizuoja kasmetinį ir neeilinį (esant poreikiui) informacijos saugos rizikos vertinimą;

21.5. užtikrina, kad Įmonė vadovaujasi informacijos saugą reglamentuojančiais teisės aktais, vertina atitiktį jų reikalavimams;

21.6. organizuoja veiklos tęstinumo valdymo plano bandymus;

21.7. teikia siūlymus ir organizuoja darbuotojų mokymus informacijos saugos klausimais;

21.8. bendradarbiauja su DAP asmens domenų apsaugos klausimais;

21.9. Per tris mėnesius po kibernetinio saugumo klausimais organizuotų mokymų organizuoja mokymų ataskaitos parengimą, kurioje turi būti nurodyta mokymų tema, dalyvių skaičius. Mokymus nurodytomis temomis Įmonė turi teisę įsigyti iš trečiųjų šalių arba organizuoti pats. Įmonė parengtą mokymų ataskaitą turi saugoti ne mažiau kaip trejus metus nuo ataskaitos patvirtinimo datos;

21.10. teikia pasiūlymus Įmonės vadovui ar jo įgaliotam asmeniui dėl:

21.10.1. Politiką įgyvendinančių teisės aktų ir kitų dokumentų priėmimo, keitimo ar panaikinimo.

21.11. Atlieka kitus įstatymų numatytas užduotis.

22. Už asmens duomenų tinkamo saugojimo užtikrinimą atsakingas Duomenų apsaugos pareigūnas (DAP).

23. Sistemų administratorius:

23.1. suteikia, keičia ir panaikina Naudotojams prieigos teises prie Įmonės Informacinių sistemų, apmoko bei konsultuoja Naudotojus;

23.2. vykdo kompiuterinių darbo vietų, veikimo koordinavimą, nustato pažeidžiamas vietas;

23.3. užtikrina kompiuterių tinklo tinkamą veikimą;

23.4. užtikrina tarnybinių stočių tinkamą veikimą;

23.5. užtikrina duomenų bazių ir duomenų bazių archyvo, atsarginio kopijavimo įrangos veikimą;

23.6. atsako už duomenų atsarginių kopijų darymą, saugojimą ir duomenų iš atsarginių kopijų atkūrimą bei saugą;

23.7. Vykdo saugumo reikalavimų atitikties nustatymą ir stebėseną, reagavimą į kibernetinius saugumo incidentus;

23.8. vykdo IT vadovo nurodymus ir pavedimus, susijusius su saugos užtikrinimu.

24. Saugumo operacijų centras (SOC):

24.1. Užtikrina nuolatinį IT infrastruktūros stebėjimą;

24.2. Incidentų nustatymą ir valdymą, remiantis Įmonės „Kibernetinių saugumo incidentų valdymo tvarka“;

24.3. Informacijos apie grėsmes rinkimą, analizę ir prevenciją;

24.4. Užtikrina informacijos teikimą;

24.5. Teikia periodines ataskaitas apie veiklą, įtraukiant grėsmių tendencijas, nustatytų incidentų statistiką, jų suvaldymo rezultatus.

25. Visi darbuotojai privalo:

25.1. laikytis informacijos saugos reikalavimų, nustatytų šioje Politikoje;

25.2. saugoti asmens duomenų paslaptį ir Įmonės Informaciją;

25.3. pasirašyti konfidencialumo sutartis ir laikytis konfidencialumo įsipareigojimų, kurie galioja visą darbo laiką Įmonėje ir nutraukus ar pasibaigus darbo ar sutartiniams santykiams;

25.4. nedelsiant pranešti apie silpnąsias vietas, pastebėtus galimus ar įvykusius informacijos saugos įvykius ir incidentus pagal nustatytą „Kibernetinių saugumo incidentų valdymo tvarką“;

25.5. naudoti informacinius išteklius, laikantis „Techninės ir programinės įrangos naudojimosi taisyklių“;

25.6. laikytis slaptažodžiams nustatytų reikalavimų.

VII. ISVS TAIKYMO SRITIS IR ĮGYVENDINIMO ETAPAI

26. Įmonėje įdiegta ISVS apima informacinių technologijų, telekomunikacijų infrastruktūros paslaugų ir programinės įrangos priežiūrą ir aptarnavimą. ISVS įgyvendinama vadovaujantis LST ISO/IEC 27001:2022 „Informacijos technologija. Saugumo metodai. Informacijos saugumo valdymo sistemos. Reikalavimai“ standartu ir kitais galiojančiais teisės aktais.
27. ISVS įgyvendinama šiais etapais:

27.1. Planavimas. Šio etapo metu numatoma ISVS politika, tikslai, procesai, susiję su rizikų valdymu ir informacijos saugos valdymu ir tobulinimu, siekiant rezultatų, atitinkančių veiklos tikslus;

27.2. Taikymas. Šio etapo metu vykdoma ISVS politika, taikomos valdymo priemonės ir procesai;

27.3. Tikrinimas. Šio etapo metu stebimas ir vertinamas taikomų ISVS procesų veikimas, atsižvelgiant į ISVS politiką, tikslus bei praktinę patirtį, o gauti rezultatai pateikiami Įmonės vadovybės vertinimui;

27.4. Plėtra. Šio etapo metu imamasi korekcinių bei prevencinių veiksmų, atsižvelgiant į ISVS vidinio audito rezultatus ir Įmonės vadovybės atliktą analizę ar kitą aktualią informaciją, siekiant užtikrinti nuolatinį ISVS tobulinimą.

VIII. PRIEIGŲ VALDYMAS

28. Prieiga prie informacinių išteklių suteikiama vadovautis „būtina žinoti" principu, t.y. subjektams (darbuotojams, rangovams, kitoms šalims, informacinėms sistemoms, ir kt.) suteikiama tik minimali, būtina veiklai, prieiga.
29. Prieigos inicijavimo, sankcionavimo ir administravimo atsakomybės turi būti atskirtos, t. y. prieigos teises patvirtinti ir prieigos teises suteikti turi skirtingi asmenys. Prieigos teisių tvirtinimą atlieka IT skyriaus vadovas, suteikimą - Sistemų administratorius.
30. Naudotojams turi būti suteikiama minimali prieiga tik prie būtinų darbo funkcijoms atlikti tinklų ir tinklo paslaugų.
31. Įmonėje turi būti nustatytos formalios naudotojų registravimo, išregistravimo ir teisių peržiūros procedūros visiems informaciniams ištekliams. Jei naudotojo pareigos Įmonėje keičiasi, ankstesnės teisės turi būti panaikinamos ir suteikiamos naujas pareigas atitinkančios teisės. Už naudotojų teisių patvirtinimą, periodinę peržiūra ir teisių panaikinimą atsakingas Sistemų administratorius. Kiekvienas Naudotojas turi būti unikaliai atpažįstamas taip

užtikrinant individualią atsakomybę už atliekamus veiksmus. Pagal technines galimybes, naudojamos kelių veiksmų tapatumo nustatymo priemonės.

32. Anoniminė prieiga leidžiama tik prie viešos informacijos.
33. Administratoriaus funkcijos turi būti atliekamos naudojant atskirą tam skirtą paskyrą, kuri negali būti naudojama kasdienėms naudotojo funkcijoms atlikti.
34. Kai prieiga prie informacinių išteklių yra nebereikalinga, nes Naudotojas išeina iš darbo, keičiasi jo pareigos ar dėl kitokių priežasčių, Naudotojo prieiga prie informacinių išteklių turi būti nedelsiant panaikinama.
35. Baigus darbą su kompiuteriu ar Naudotojui pasitraukiant iš kompiuterinės darbo vietos, turi būti imamasi priemonių, kad su informacija, negalėtų susipažinti pašaliniai asmenys: atsijungiama nuo informacinių išteklių, įjungiama ekrano užsklanda su slaptažodžiu.
36. Naudotojui neatliekant jokių veiksmų 10 min., kompiuteris turi užsirakinti, kad toliau naudotis juo būtų galima tik pakartotinai patvirtinus tapatybę.
37. Prisijungimo slaptažodžių reikalavimai:
    37.1. Slaptažodis turi būti sudarytas iš raidžių, skaičių ir specialiųjų simbolių;
    37.2. Slaptažodžiams sudaryti neturi būti naudojama asmeninio pobūdžio informacija (pavyzdžiui, gimimo data, šeimos narių vardai ir panašiai) ar prisijungimo vardas;
    37.3. Draudžiama slaptažodžius atskleisti kitiems asmenims.
38. Informaciniai ištekliai, patvirtinantys Naudotojo tapatumą, turi neleisti automatiškai išsaugoti slaptažodžius interneto naršyklėse ar kitose duomenų suvedimo formose, turinčiose išsaugojimo funkciją.
39. Turi būti nustatytas didžiausias leistinas Naudotojo mėginimų įvesti teisingą slaptažodį skaičius (ne daugiau kaip 3 kartai).
40. Keičiant slaptažodį, Naudotojui neturi leisti sudaryti slaptažodžio iš buvusių 3 paskutinių slaptažodžių.
41. Pirmąkart jungiantis prie informacinių išteklių, turi būti reikalaujama, kad Naudotojas pakeistų slaptažodį.
42. Turi būti patvirtinti asmenų, kuriems suteiktos administratoriaus teisės prisijungti prie Informacinių išteklių, sąrašai, periodiškai peržiūrimi Kibernetinio saugumo vadovo.
43. Turi būti vykdoma Administratorių paskyrų kontrolė:
    43.1. Periodiškai tikrinama, ar nėra nereikalingų/nebegaliojančių Administratoriaus paskyrų;
    43.2. Turi būti registruojami visi prašymai suteikti/panaikinti/pakoreguoti prieigos teises prie informacinių išteklių.
44. Draudžiama Informacinių išteklių techninėje ir programinėje įrangoje naudoti gamintojo nustatytus slaptažodžius, jie turi būti pakeisti į naujus.
45. Įmonėje turi būti taikoma „švaraus stalo" tvarka - draudžiama palikti be priežiūros dokumentus (pvz.: darbo kabinete ant stalo pasibaigus darbo laikui) su svarbia informacija (pvz.: informacija skirta vidiniam naudojimui, komercinės ar technologinės paslaptys, asmens duomenys ir kt.). Svarbūs dokumentai turi būti tinkamai apsaugoti nuo nesankcionuotos prieigos.
46. Išorinių šalių nuotoliniai prisijungimai galimi tik apibrėžtam išorinės šalies darbuotojų skaičiui, pasirašiusiems atitinkamus konfidencialumo įsipareigojimus.
47. Prieigų valdymo procedūra detaliau dokumentuota „Prieigos prie informacinių sistemų ir jose saugomų duomenų tvarkos aprašas".

IX. KELIŲ VEIKSNIŲ TAPATUMO NUSTATYMO SPRENDIMAI

48. Įmonė nustato kelių veiksnių tapatumo nustatymo, saugių balso, vaizdo ir teksto ryšių bei saugių avarinių sistemų naudojimo organizacijos viduje taisykles, siekiant užtikrinti informacijos saugumą ir atitiktį.
49. Įmonė dokumentuoja naudojamus kelių veiksnių autentifikavimo sprendimus bei tolesnį naudotojo patikrinimą, atliekamą siekiant aptikti neteisėtą prieigą.
50. Užtikrinant ryšių saugumą, užtikrinamos priemonės komunikacijos vykdymui, prieigos kontrolei bei dokumentavimui.
51. Įmonė privalo užtikrinti, kad avarinio ryšio kanalai būtų nepriklausomi nuo pagrindinės infrastruktūros (pvz., radijo ryšys, palydovinis ryšys) bei nuolat testuojami.
52. Detalesnė tvarka kaip įgyvendinami reikalavimai dėl tapatumo nustatymo sprendimų, ryšių priemonių saugumo užtikrinimo ar avarinės sistemos naudojimo taisyklės įtvirtintos Įmonės patvirtintoje „Kelių veiksnių tapatumo nustatymo sprendimų, saugių balso, vaizdo ir teksto ryšių bei saugių avarinių sistemų naudojimo tvarkoje“.

X. REIKALAVIMAI DARBUOTOJAMS

53. Įmonėje turi būti nustatyti ir į atitinkamus vidaus dokumentus (darbo sutartis, darbo tvarkos taisykles, pareiginius nuostatus, konfidencialumo susitarimus ir kt.) įtraukti darbuotojams (rangovams, paslaugų teikėjams, bei kitiems išorinių šalių atstovams) keliami saugos reikalavimai, prievolės ir atsakomybės. Reikalavimuose turi būti numatytos prievolės:
    53.1. laikytis Įmonės „Kibernetinės saugos politikos“ ir ją įgyvendinančių Įmonės tvarkų reikalavimų;
    53.2. saugoti Įmonės informacinius išteklius nuo nesankcionuotos prieigos, atskleidimo, modifikavimo ar sunaikinimo;
    53.3. informuoti atsakingus asmenis apie saugumo incidentus ar įvykius.
54. Prieš įdarbinant naują darbuotoją Įmonėje turi būti įsitikinta kandidato pateiktos informacijos autentiškumu (pvz.: pateikiami kvalifikaciją patvirtinančių dokumentų originalai, įsitikinama rekomendacinių laiškų autentiškumu), bei patikrinama kita, kandidato pateikta, reikšminga informacija.
55. Prieiga prie Įmonės informacinių išteklių naujam darbuotojui suteikiama tik darbuotojui pasirašytinai susipažinus su Politika, ją įgyvendinančiomis Įmonės tvarkomis ir kitais informacijos saugos reikalavimais bei darbuotojo atsakomybe.
56. Nutraukus darbo santykius su darbuotoju ar keičiantis darbuotojo pareigoms prieiga prie informacinių sistemų/išteklių turi būti nedelsiant panaikinama. Įmonėje turi būti įgyvendinta tvarka, kuria užtikrinama, kad darbuotojai grąžina visus suteiktus fizinius informacinius išteklius iki nutraukiant darbo sutartį.

XI. MOKYMAI

57. Kibernetinio saugumo vadovas atsakingas už reguliarų Darbuotojų mokymų vykdymą bei kito pobūdžio edukaciją.
58. Kibernetinės higienos ir Asmens duomenų saugos mokymai turi būti atliekami 1 kartą į metus, įtraukiant naujus darbuotojus. Įmonė išsaugo mokymų įrodymus bei dalyvių sąrašus.
59. Per tris mėnesius po kibernetinio saugumo klausimais organizuotų mokymų turi būti parengta mokymų ataskaita, kurioje turi būti nurodyta mokymų tema, dalyvių skaičius. Mokymus

nurodytomis temomis Įmonė turi teisę įsigyti iš trečiųjų šalių arba organizuoti pats. Įmonė parengtą mokymų ataskaitą turi saugoti ne mažiau kaip trejus metus nuo ataskaitos patvirtinimo datos.

60. Darbuotojų edukacijai stiprinti, ne rečiau nei 4 kartus į metus, vykdomos socialinės inžinerijos atakų simuliacijos.
61. Įgyvendinus socialinės inžinerijos simuliacijos ataką parengiama ataskaita bei Darbuotojams išplatinamos aktualiausios rekomendacijos.

XII. FIZINIS SAUGUMAS

62. Fizinis saugumas Įmonėje organizuojamas atsižvelgiant į patalpų, kuriose organizuojamas darbas ar laikoma kritinės svarbos infrastruktūra pobūdį bei patekimo į jas galimybes.
63. Visos patalpos, kuriose yra svarbi informacinių išteklių įranga (pvz., tarnybinių stočių patalpos, duomenų centrai, ryšių mazgai) ar duomenys (pvz., dokumentų archyvai), (toliau - padidinto saugumo zonos) turi būti identifikuotos ir nurodytos Tinklų ir informacinių sistemų fizinės prieigos reikalavimuose.
64. Patekimas į tarnybines patalpas/pastatus leidžiamas tik sankcionuotam personalui. Pašaliniai asmenys, esantys tarnybinėse patalpose (lankytojai, rangovai ir kt.), turi būti lydimi Įmonės darbuotojo.
65. Padidinto saugumo zonose turi būti numatytos prieigos kontrolės priemonės, kurios ribotų patekimą tik sankcionuotam personalui.
66. ITT įranga turi būti apsaugota nuo palaikymo sistemų (elektros energijos ir vandens tiekimas, nuotekos, šildymas, vėdinimas ir oro kondicionavimas) sutrikimų.
67. Tarnybinių stočių patalpos, spinta ir elektra prižiūrimos pagal „Tinklų ir informacinių sistemų fizinės prieigos reikalavimus“.
68. Įranga turi būti prižiūrima vadovaujantis įrangos gamintojo nurodytomis instrukcijomis ir nurodytu periodiškumu. Priežiūrą gali atlikti tik sankcionuotas personalas. Turi būti vedami gedimų registravimo žurnalai.
69. Detalesni reikalavimai pateikiami įmonės patvirtintoje tvarkoje „Tinklų ir informacinių sistemų fizinės prieigos reikalavimai“.

XIII. TINKLO VALDYMO PRIEMONĖS

70. Įmonėje turi būti įgyvendintos tinkamos kompiuterių tinklo kontrolės priemonės:
    - 70.1. Įmonės darbuotojų kompiuterinis tinklas turi būti atskirtas nuo serverių tinklo;
    - 70.2. Prieiga prie Įmonės valdomo kompiuterinio tinklo ir tinklo įrangos privalo būti identifikuota ir patvirtinta (vykdoma griežta įrenginių kontrolė);
    - 70.3. Turi būti užtikrinama apsauga nuo nesankcionuotos loginės ir fizinės prieigos prie kompiuterinio tinklo įrenginių valdymo (diagnostikos, konfigūravimo) prievadų. Visi nebūtini veiklai tinklo įrenginių valdymo prievadai turi būti išjungti.
71. Neatpažintų įrenginių darbas tinkle turi būti blokuojamas pagal nutylėjimą iki tokie įrenginiai pažymimi sistemoje kaip patvirtinti.
72. Informacija apie neatpažintus įrenginius turi būti automatiškai išsiunčiama atsakingam darbuotojui.
73. Turi būti vykdomas tinklo įrangos konfigūracijų rezervinis kopijavimas po kiekvieno pakeitimo tinklo konfigūracijoje, bet ne vėliau kaip per 1 savaitę nuo pakeitimų atlikimo.
74. Tinklo įrenginių administravimas gali būti vykdomas naudojant tik saugius protokolus,

pavyzdžiui HTTPS, SSH.

75. Ugniasienės privalo žurnalizuoti tinklo srautus (šaltinio adresas, paskirties adresas, protokolas/prievadas, laikas ir trukmė).
76. Ugniasienės privalo blokuoti visą tinklo srautą (angl. „deny by default“) ir praleisti tik taisyklių pagalba įtrauktas išimtis.
77. Įmonės duomenų tinklas turi būti segmentuojamas į skirtingų saugumo lygių zonas. Ugniasienėmis turi būti atskirtos: sistemų prieinamų iš išorės grupės; vidinių sistemų grupės; naudotojų grupės. Duomenų srautai tarp skirtingų saugumo zonų turi būti kontroliuojami ir leidžiami tik minimalūs, būtini veiklai.
78. Turi būti išjungti nenaudojami TCP (angl. Transmission Control Protocol) / UDP (angl. User Datagram Protocol) ar QUIC(angl. Quick UDP Internet Connections) prievadai.
79. Turi būti registruojami duomenys apie visus įrenginius turinčius IP adresus: kompiuteriai, telefonai, serveriai, kameros, spausdintuvai, tinklo įrenginiai, IP telefonai, kita periferija.
80. Bevielis ryšys turi būti saugiai šifruojamas.
81. Turi būti sudaryta ir patvirtinta vieninga saugi bevielio ryšio komunikacijų įrangos (Wi-Fi) konfigūracija. Įmonės vidaus bevielio tinklo apsaugai turi būti taikomas WPA3 (angl. „Wi-Fi Protected Access 3“) arba saugesnis protokolas bei naudojamas šifravimas mažiausiai 256 bitų ilgio raktu.
82. Prieiga prie Įmonės bevielio tinklo turi būti leidžiama tik autorizuotiems naudotojams.
83. Nuotoliniam prisijungimui gali būti naudojami tik saugūs prisijungimo metodai bei tinkamos apsaugos priemonės, tokios kaip VPN .
84. Nuotolinis prisijungimas per VPN turi būti suteikiamas ribotam laikotarpiui.
85. Turi būti atliekamas nuolatinis tinklo parametrų ir saugumo įvykių stebėjimas.
86. Visi svarbūs duomenys perduodami tinklais turi būti saugiai šifruojami.
87. Taikomos saugos priemonės susijusios su interneto ryšio naudojimu:
88. Prieiga iš interneto turi būti saugoma ugniasienės pagalba;
89. Įmonė gali, be išankstinio perspėjimo, blokuoti interneto resursus, jei šie resursai yra/buvo nesaugūs ar jie neatitinka keliamų saugumo reikalavimų bei sukelia grėsmes Įmonės tinklams (pvz. DDoS atakos, spam žinutės ir kt.).
90. Įmonė gali blokuoti interneto resursus, kurie tiesiogiai ar netiesiogiai sukuria didelę papildomą tinklo/sistemų apkrovą ar gali kitaip įtakoti Įmonės veiklą.
91. Įmonė gali riboti prieigą prie kitų el. pašto sistemų/portalų, kurie nesiejami su darbuotojo atliekamomis darbo funkcijomis.
92. Papildomi reikalavimai bevielės prieigos taškams:
    92.1. Kas mėnesį privalo būti vykdoma reguliari belaidės prieigos taškų patikra.
93. ne rečiau kaip kartą per mėnesį administratoriaus turi būti atliekama ugniasienių užfiksuotų įvykių analizė. Ugniasienės užfiksuotų įvykių ataskaita reguliariai turi būti pateikiama ir kibernetinio saugumo vadovui.
94. turi būti uždraustas SNMP (angl. „Simple Network Managment Protocol“) protokolo naudojimas belaidėje sąsajoje, išskyrus protokolo saugios versijos naudojimą stebėsenos tikslais;
95. turi būti uždrausti visi nebūtini bevielių įrenginių valdymo protokolai.

XIV. INFORMACINIŲ IŠTEKLIŲ VALDYMAS

96. Įmonėje leidžiama naudoti tik gamintojų palaikomą aparatinę įrangą. Turi būti naudojama aparatinės įrangos gamintojo išleista naujausia programinė-aparatinės įrangos versija, turinti

visas saugumo pataisas.

97. Įmonės aparatinėje įrangoje turi būti naudojama kompetentingų specialistų paruošta ir įdiegta operacinė sistema.
98. Operacinių sistemų naudotojams turi būti panaikinti visi, nebūtini veiklai OS komponentai (servisai, taikomosios programos, sisteminės priemonės).
99. Darbo vietų, tarnybinių stočių bei kitos įrangos operacinės sistemos turi būti apsaugotos nuo nesankcionuotos prieigos. Operacinės sistemos starto metu turi būti apsaugotos nuo alternatyvių OS paleidimo metodų (pvz.: startas iš USB, CD/DVD laikmenų). Prieiga prie BIOS nustatymų apsaugota saugiu slaptažodžiu.
100. Naudojamose operacinėse sistemose turi būti įgyvendinti slaptažodžių sudėtingumo ir keitimo reikalavimai. Slaptažodžių saugojimui naudojami tik patikimi ir saugūs šifravimo bei maišos algoritmai.
101. Įmonės aparatinėje įrangoje turi būti naudojama sankcionuota, leistinuose sąrašuose esanti, programinė įranga. Turi būti įdiegtos programinės įrangos gamintojo išleistos kritinius ir svarbius programinės įrangos saugumo pažeidžiamumus taisančios pataisos.
102. Visi Įmonės informaciniai ištekliai turi būti apskaitomi „Informacinių išteklių registre“ ir priskirti konkretiems asmenims – informacinių išteklių savininkams.
103. Informaciniuose ištekliuose turi būti įdiegta antivirusinė programinė įranga, kuri turi reguliariai atsinaujinti. Jei nėra galimybės informaciniuose ištekliuose įdiegti antivirusinės programos, informaciniai ištekliai turi būti atjungti nuo interneto, informacija ir duomenys perkeliami į šiuos informacinius išteklius prieš tai turi būti patikrinami ar juose nėra kenksmingo kodo.
104. Įmonės informacija turi būti klasifikuojama pagal informacijos svarbą ir poreikį jos saugai pagal įmonėje patvirtintus „Informacijos klasifikavimo reikalavimus“.
105. Visi Įmonės darbuotojai turi būti pasirašytinai susipažinę ar elektroninių priemonių pagalba patvirtinę susipažinimą su konfidencialios informacijos apibrėžimu, reikalavimais konfidencialios informacijos saugojimui ir savo atsakomybe.
106. Internetu pasiekiami informaciniai ištekliai turi tenkinti šiuos reikalavimus:
    106.1. Perduodami duomenys turi būti šifruojami;
    106.2. Šifravimui naudojami skaitmeniniai sertifikatai privalo būti išduoti patikimų sertifikavimo tarnybų. Sertifikato raktas turi būti ne trumpesnis kaip 2048 bitų;
    106.3. Perduodamų duomenų šifravimu turi būti naudojamas TLS (angl. Transport Layer Security) standartas;
    106.4. Turi būti naudojamos apsaugos nuo pagrindinių per tinklą vykdomų atakų: SQL įskverbties (angl. SQL injection), įterptinių instrukcijų atakų (angl. Cross-site scripting), atkirtimo nuo paslaugos (angl. DOS), paskirstyto atsisakymo aptarnauti (angl. DDOS) ir kitų, priemonės; pagrindinių per tinklą vykdomų atakų sąrašas skelbiamas Atviro tinklo programų saugumo projekto (angl. The Open Web Application Security Project (OWASP)) interneto svetainėje www.owasp.org;
    106.5. Turi būti naudojama informacinių išteklių naudotojo įvedamų duomenų tikslumo kontrolė (angl. Validation);
    106.6. Tarnybinė stotis, kurioje yra informacinių išteklių, neturi rodyti naudotojui klaidų pranešimų apie svetainės programinį kodą ar tarnybinę stotį;
    106.7. Informacinių išteklių saugumo priemonės turi gebėti automatiškai uždrausti prieigą prie tarnybinės stoties iš IP adresų, vykdžiusių grėsmingą veiklą (nesankcionuoti mėginimai prisijungti, įterpti SQL intarpus ir panašiai), Įmonė tai įgyvendina per Išorinės

šalies įdiegtą sprendimą;

106.8. Tarnybinė stotis, kurioje yra informaciniai ištekliai, turi leisti tik informacinių išteklių funkcionalumui užtikrinti reikalingus HTTPS metodus;

106.9. Turi būti uždrausta naršyti informacinių išteklių aplankuose (angl. Directory browsing).

107. Įmonės informacinėse sistemose turi būti registruojama ir ne mažiau kaip 12 mėnesių saugoma su informacine sistema atliktų veiksmų informacija:

107.1. prisijungusio naudotojo ar administratoriaus identifikatoriai;

107.2. esminių įvykių laikai;

107.3. kompiuterio, iš kurio jungiamasi, informacija;

107.4. sėkmingos ir nesėkmingos prieigos įrašai;

107.5. administracinių teisių naudojimas;

107.6. sistemos konfigūracijos keitimas, sisteminių priemonių naudojimas;

107.7. resursai, prie kurių buvo suteikta prieiga; sisteminiai pranešimai.

108. Veiksmų žurnaliniai įrašai turi būti apsaugoti nuo neautorizuoto modifikavimo ir ištrynimo.

109. Visų Įmonės informacinių sistemų laikrodžiai turi būti sinchronizuoti pagal sutartą tikslų laiko šaltinį. Naudotojams keisti sistemos laiką turi būti draudžiama.

110. Įgyvendinant šio skyriaus reikalavimus laikomasi Įmonės patvirtintos “Kriptografijos ir šifravimo naudojimo tvarkos”.

XV. INFORMACINIŲ IŠTEKLIŲ ĮSIGIJIMAS IR PRIEŽIŪRA

111. Prieš įsigyjant, kuriant naujus ar plečiant esamus informacinius išteklius (operacines sistemas, ITT infrastruktūros elementus, taikomąją programinę įrangą, ITT paslaugas), turi būti nustatyti ir dokumentuoti informacijos saugos reikalavimai. Saugumo rizikų įvertinimas turi būti atliekamas sistemų inicijavimo stadijoje.

112. Įsigyjami ar kuriami informaciniai ištekliai privalo užtikrinti apdorojamų duomenų tikslumą.

113. Informacinių sistemų kūrimo, testavimo ir darbinės (eksploatacinės) aplinkos turi būti atskirtos. Programinės įrangos ir duomenų perkėlimo iš vienos aplinkos į kitą procesas turi būti nustatytas ir dokumentuotas.

114. Taikomosios programinės įrangos testavimą ir diegimą atlieka specialistai laikydamiesi dokumentuotų procedūrų. Informacinių išteklių funkcionalumo testavimui turi būti naudojama testavimo aplinka, kuri turi būti saugoma laikantis tų pačių reikalavimų kaip ir darbinė aplinka.

115. Prieiga prie informacinių išteklių išeitinių tekstų turi būti apribota tik sankcionuotiems asmenims, kuriems ji būtina pagal darbo pobūdį.

116. Nauji informaciniai ištekliai turi būti integruoti su esamomis saugos sistemomis (pvz. žurnalinių įrašų centralizuoto surinkimo sistema, pažeidžiamumų valdymo sistema, atnaujinimų valdymas ir pan.).

117. Įgyvendinant informacinių išteklių parengimą pakartotiniam naudojimui, nurašymui ar naikinimui, siekiant išvengti konfidencialios informacijos atskleidimo, įsitikinama, kad visi juose esantys duomenys yra saugiai panaikinti remiantis Įmonės patvirtintu „Duomenų naikinimo ir šalinimo tvarkos aprašu“.

XVI. KEITIMŲ VALDYMAS

118. Keitimų valdymo tikslas sinchronizuoti ir kontroliuoti visus Informacinėse sistemose, kuriose apdorojama Įmonės Informacija ir Asmens duomenys, atliekamus pakeitimus. Tai yra svarbi saugumo priemonė, nes nesėkmingas pakeitimų įgyvendinimas gali sukelti neteisėtą duomenų atskleidimą, pakeitimą ar sunaikinimą.
119. Informacinių išteklių pakeitimai turi būti atliekami laikantis „IT keitimų valdymo apraše“ nurodytos procedūros. Turi būti užtikrinta, kad prieš atliekant pakeitimus sistemoje įvertinamas galimas poveikis sistemoms. Keitimo inicijavimo ir įgyvendinimo atsakomybės turi būti atskirtos, keitimai turi būti dokumentuojami.
120. Poreikis keitimams gali iškilti dėl įvairių priežasčių, įskaitant, bet neatsiribojant žemiau išvardintiems:
    120.1. Naudotojų prašymai;
    120.2. tiekėjų paslaugų pasikeitimai;
    120.3. techninės ar programinės įrangos atnaujinimai;
    120.4. naujos techninės ar programinės įrangos diegimai;
    120.5. infrastruktūros pasikeitimai.
121. Identifikuoti keitimų poreikiai suskirstomi į kategorijas pagal svarbą (aukštas, vidutinis, žemas) ir skubumą (skubus, vidutinis, neskubus).
122. Įvertinama, reikiamų keitimų įtaką Įmonės veiklai ir techninei įrangai, nustatomi galimi trikdžiai, Naudotojų papildomo apmokymo poreikis ir pan. Pagal šią analizę nustatoma kiekvieno keitimo įtaka (aukšta, vidutinė, žema).
123. Pagal nustatytą svarbą ir skubumą nustatomi keitimo prioritetai.
124. Pagal nustatytus keitimo prioritetus nustatomos keitimų sąrašas, jų atlikimo datos, reikiamas biudžetas ir galimi vykdytojai. Visų pasirinktų vykdyti keitimų atlikimą organizuoja ir prižiūri Sistemų administratorius, kuris kontroliuoja, kad keitimai būtų atlikti pagal nustatytus terminus ir atitiktų taikomus kokybės reikalavimus.
125. Keitimai planuojami ir testuojami naudojant atskirą testavimui skirtą aplinką, kurioje esantys asmens duomenys turi būti naudojami vadovaujantis Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymu bei BDAR.
126. Patvirtinus sėkmingo testavimo rezultatus, diegimui gamybinėje aplinkoje turi būti paruoštas diegimo paketas, numatytos diegimo procedūros.
127. Įmonė užtikrina, kad visi Informacinių sistemų pakeitimai būtų stebimi ir registruojami Sistemų administratoriaus.
128. Keitimų vykdymo procedūra aprašyta „IT keitimų valdymo tvarkos apraše“.

XVII. KOMPIUTERINĖS DARBO VIETOS IR MOBILŪS ĮRENGINIAI

129. Įmonės kompiuterinėje įrangoje turi būti įdiegta legali, gamintojo palaikoma ir Įmonės leidžiama operacinė sistema bei programinė įranga.
130. Kompiuterinių darbo vietų naudotojai negali turėti kompiuterio administravimo teisių.
131. Standartinės, gamintojo sukurtos, vartotojų paskyros privalo būti ištrintos arba išjungtos, įskaitant Guest/Anonymous paskyras.
132. Nenaudojami procesai arba nenaudojami operacinės sistemos programiniai paketai privalo būti išjungti arba ištrinti.
133. Kompiuterinėse darbo vietose turi būti diegiamos gamintojo išleistos operacinės sistemos ar programinės įrangos pataisos.
134. Ne rečiau kaip kartą per mėnesį kompiuterinės darbo vietos turi būti atnaujinamos.
135. Windows operacinėje sistemoje standartinis kompiuterio diskų dalinimasis (angl.

136. „Administrative Share“ arba „C$“) turi būti išjungtas.
137. Administravimo tikslais jungtis nuotoliniu būdu prie Įmonės darbuotojų kompiuterių leidžiama tik, jei:
    137.1. yra gautas kompiuterio naudotojo sutikimas;
    137.2. yra registruotas atitinkamas kreipinys;
    137.3. yra centralizuotai kaupiami žurnaliniai įrašai apie tokius prisijungimus.
138. Visų Įmonės nešiojamų kompiuterių kietajame diske esantys duomenys privalo būti šifruojami.
139. Įmonėje turi būti išjungtas failų automatinio paleidimo (angl. „auto-run“) funkcionalumas į kompiuterius įjungus USB/CD/DVD/Flash/FireWire įrenginius.
140. USB/išorinių HDD/CD/DVD/Flash atmintinių naudojimas yra draudžiamas. Išimtis nustato Įmonės vadovas arba jo įgaliotas asmuo.
141. Kompiuterinės darbo vietos privalo būti sukonfigūruotos taip, kad darbuotojas negalėtų išjungti ar pakeisti sisteminės ar saugos priemonių programinės įrangos, tokios kaip antivirusinė programinė įranga, nustatymų.
142. Kompiuterinėse darbo vietose turi būti įdiegta antivirusinė programa, kuri:
    142.1. pasileistų ir būti aktyvi sistemos paleidimo ir darbo metu;
    142.2. turėtų aktyvuotą realaus laiko grėsmių stebėjimą bei blokuotų galimus kenkėjiškus veiksmus;
    142.3. tikrintų ar yra atnaujinimų ne rečiau kaip kas 24 val. ir sudiegtų esamus atnaujinimus nedelsiant;
    142.4. automatiškai skanuotų visą sistemą ne rečiau kaip kas 7 dienas;
    142.5. būtų administruojama centralizuotai;
    142.6. palaikytų priverstinius atnaujinimus iš centralizuoto valdymo serverio;
    142.7. automatiškai skanuotų bylas prieš jas atidarant ar paleidžiant.
143. Draudžiama dirbti su konfidencialia įmonės informacija viešosiose vietose.
144. Dirbant su konfidencialia informacija ne viešose vietose per telekomunikacinių įmonių tinklus ji privalo būti perduodama saugiu šifruotu kanalu (pvz., VPN) arba užšifruojant perduodamą informaciją.
145. Nešiojami įrenginiai, kuriuose yra slapta ir/arba konfidenciali Įmonės informacija, negali būti paliekami be priežiūros, jei patalpos kuriose paliekama įranga nėra fiziškai apsaugotos nuo pašalinių asmenų prieigos.
146. Draudžiama dalintis įmonės nešiojamais kompiuteriais ir mobiliais įrenginiai su kitais asmenimis (kolegomis, svečiais, draugais ar šeimos nariais) ir, pvz., mobilaus telefono baterijos pakrovimo tikslu, jungti prie svetimo kompiuterio.
147. Kelionėse (pvz., lėktuve, traukinyje, autobuse ir pan.) saugoti nešiojamus kompiuterius ir mobilius įrenginius, neatiduoti transportavimui į bagažą.
148. Visuose mobiliuose įrenginiuose privalo būti įdiegta slaptažodžiu ar PIN kodu apsaugota prieiga. Slaptažodžiai privalo būti periodiškai keičiami. Nešiojamo kompiuterio ar mobilaus įrenginio netekimo atveju (pametus, pavogus ir pan.) darbuotojas nedelsiant privalo informuoti savo tiesioginį vadovą.
149. Detalesni saugumo reikalavimai pateikiami „Techninės ir programinės įrangos naudojimosi taisyklėse“.

XVIII. INTERNETO IR ELEKTRONINIO PAŠTO NAUDOJIMAS

150. Draudžiama naudotis internetu ir elektroniniu paštu sukčiavimo, reklamos ir asmeninės

finansinės naudos tikslais, dalyvauti interneto lažybose ir azartiniuose lošimuose, lankytis pornografiniuose tinklalapiuose.

151. Draudžiama Įmonės sukurtos paskyros duomenis naudoti trečiųjų šalių interneto svetainėse.
152. Elektroninis paštas yra ryšio priemonė, skirta tiesioginėms funkcijoms atlikti ir naudotojai turi naudoti šią priemonę atsakingai, veiksmingai ir teisėtais tikslais.
153. Draudžiama elektroniniu paštu siusti Įmonės konfidencialią informaciją, jei dėl tokios informacijos siuntimo nebuvo gautas tiesioginio vadovo leidimas.
154. Draudžiama elektroniniu paštu siųsti Naudotojo tapatybės patikrinimui naudojamą informaciją (pavyzdžiui, slaptažodį), išskyrus atvejus, kai taikomos papildomos saugumo priemonės.
155. Neatidarinėti laiškų, jeigu siuntėjas nėra aiškus, prie jų pridėtas failas ar neaiškus laiško
156. turinys.
157. Draudžiama spausti ant elektroniniame laiške esančių nuorodų, jei laiško siuntėjas yra
158. nežinomas.
159. Detalesni saugumo reikalavimai pateikiami „Techninės ir programinės įrangos naudojimosi taisyklėse“.

XIX. NUOTOLINIO DARBO REIKALAVIMAI

160. Darbuotojams prisijungti prie Įmonės vidinio tinklo ir dirbti nuotoliniu būdu galima tik gavus Tiesioginio vadovo leidimą. Jungiantis nuotoliniu būdu, Naudotojai turi būti autorizuoti ir prisijungimas galimas tik naudojant šifruotus ryšio kanalus (VPN).
161. Tretiesiems asmenims draudžiama naudotis Įmonės Technine įranga, kuri yra skirta nuotoliniam darbui.
162. Dirbant nuotoliniu būdu, turi būti pasirinkta saugi fizinė aplinka, kurioje nebūtų galima atskleisti konfidencialios ir vidinės Informacijos neautorizuotiems asmenims, tame tarpe ir šeimos nariams ar draugams.
163. Paliekant įrangą neprižiūrimą, ji turi būti paliekama saugiai (žmonių keliamos, aplinkos keliamos grėsmės), užtikrinant jos ir joje esančios Informacijos saugumą. Negalima prie įrangos jungti Sistemų administratoriaus neautorizuotą įrangą, diegti programinę įrangą, palikti neužrakinto darbalaukio.
164. Nuotoliniu būdu dirbančių Darbuotojų įranga turi atitikti Įmonės nustatytus nuotolinės įrangos standartus (įdiegtos ir atnaujintos antivirusinės programos, sudiegti visi naudojamos programinės įrangos atnaujinimai, įjungta OS ugniasienė, ekrano užsklandos įsijungimo laikas, laikomasi „kriptografijos ir šifravimo priemonių naudojimo reikalavimų“ ir pan.).
165. Draudžiama jungtis prie nepatikimų WiFi ar kt. tinklų (viešos WiFi prieigos taškai, nedraugiškų šalių interneto tinklai (ne NATO valstybės).
166. Visa Informacija, sukurta nuotoliniu būdu, yra Įmonės nuosavybė.
167. Visi išoriniai prisijungimai kontroliuojami, vykdomos sesijos gali būti įrašomos.
168. Detalią nuotolinio darbo tvarką ir taisykles numato „Nuotolinio darbo tvarka“.

XX. SAUGUMO OPERACIJŲ CENTRAS (SOC)

169. Kibernetinio saugumo stebėsenai Įmonė pasitelkia SOC komandą, kuri užtikrina IT infrastruktūros priežiūrą - įtartinos veiklos stebėjimas per žurnalus, tinklo srautą ar kitus resursus, incidentų stebėseną, klasifikavimą ir valdymą, grėsmių analizę bei prevenciją ir

atlieka kitas priskirtinas funkcijas.

170. Paskiriant ar pasirenkant SOC komandą aiškiai apibrėžiamos komandos atsakomybės, komandos narių vaidmenys. Atveja, kai SOC komanda išorinis paslaugų teikėjas paslaugų teikimo sutartyje tiksliai nustatomi išorinės šalies įsipareigojimai, reakcijos laikas, prieinamumas, taikomos saugumo priemonės bei laikomasi Įmonėje patvirtintos darbo su išorinėmis šalimis tvarkos.

171. Kibernetinio saugumo stebėsenai Įmonė naudoja naujausias saugumo tendencijas užtikrinančius įrankius ar sprendimus, įskaitant, bet neapsiribojant – SIEM, EDR, XDR, NDR, IPS,NAC. Visi naudojami techniniai sprendimai nuolat prižiūrimi ir atnaujinami.

172. SOC komanda teikia periodines ataskaitas apie komandos veiklą IT skyriaus vadovui ir Kibernetinio saugumo vadovui, ataskaitose pateikiant išsamius duomenis apie:

172.1. patirtų incidentų statistiką;

172.2. išanalizuotas grėsmių tendencijas;

172.3. rekomendacijas prevenciniams veiksmams.

173. Įmonė užtikrina, kad SOC komandos kvalifikacija būtų nuolat keliama ir stiprinama, bei pačios SOC veikla testuojama ir išbandoma. Testavimai atliekami periodiškai bent 1 kartą per metus. SOC pasitelkimas, atsakomybės bei kiti klausimai dokumentuojami Įmonės patvirtintame „Saugumo operacijų centro valdymo tvarkoje“.

XXI. INCIDENTŲ VALDYMAS

174. Kibernetinių saugumo incidentų valdymo organizavimą Įmonės lygmeniu užtikrina IT skyriaus vadovas.

175. Įmonė užtikrina, kad Saugumo operacijų centro funkcijos saugos incidentų metu nebūtų pavedamos Įmonės arba paslaugų teikėjo darbuotojui, atsakingam už tinkamą to Įmonės tinklų ir (ar) informacinių sistemų veiklą.

176. Apie visus incidentus, aptiktas saugumo spragas, silpnas saugumo vietas nedelsiant turi būti pranešama Kibernetinio saugumo vadovui ar IT skyriaus vadovui. Visi Įmonės darbuotojai, rangovai ir kiti susiję asmenys turi būti informuoti apie savo pareigą pranešti apie saugumo incidentus, aiškiai nurodant kokiomis priemonėmis ir kas yra informuojamas apie incidentus.

177. Incidentai įmonėje nustatomi SOC arba Įmonės darbuotojų:

177.1. Atveju, kai incidentą įtaria ar patiria Įmonės darbuotojai, pranešdami apie incidentą “JIRA” sistemoje Darbuotojai turi pateikti:

177.1.1. pranešėjo vardas, pavardė, kontaktinis telefono numeris ir el. pašto adresas;

177.1.2. įvykio metu atliktos veiklos aprašymas (pvz., buvo atidarytas el. pašto priedas, buvo rodoma svetainė, pradėtas vykdomasis failas ir kt.);

177.1.3. incidento aptikimo laikas, glaustas situacijos aprašymas kartu su paskelbto ištekliaus pridėtais duomenimis (pvz., kompiuterio numeris, pašto dėžutės pavadinimas, tinklo tarnybos pavadinimas, interneto adresas ir kt.);

177.1.4. kita informacija, įskaitant neatitikimo ar pažeidimo tipą, veiksmo klaidą, ekrano žinutes, keistą elgesį ir kt..

177.2. Atveju, kai incidentą nustato SOC, apie incidentą informuojamas IT skyriaus vadovas ir Kibernetinio saugumo vadovas, pateikiant pranešimą visiems priskirtiems Sistemos administratoriams, pateiktais kontaktiniais duomenimis, pateikiant išsamius duomenis apie įvykusį incidentą. Tolesni veiksmai suderinami pagal Kibernetinio saugumo incidentų valdymo tvarką.

178. Saugumo incidentai ir įvykiai turi būti sistemingai ir nuosekliai valdomi, užtikrinant

reikiamą reagavimą ir incidentų poveikio mažinimą.

179. Visi kibernetinio saugumo incidentai valdomi pagal nustatytą „Kibernetinio saugumo incidentų valdymo planą“.

XXII. ATSARGINIS KOPIJAVIMAS

180. Siekiant užtikrinti informacinių išteklių atstatymą įvykus sutrikimui, turi būti atliekamas visų svarbių informacinių išteklių atsarginis kopijavimas.
181. Už atsarginį kopijavimą atsakingas Sistemų administratorius.
182. Informacinių išteklių konfigūracijos nustatymų atsarginės kopijos turi būti daromos nedelsiant, atlikus IT keitimus arba ne rečiau nei kartą per mėnesį.
183. Informacijos ir duomenų kopijos turi būti daromos ne rečiau kaip kartą per savaitę.
184. Atsarginės kopijos saugomos atskiroje patalpoje ir geografiškai nutolusioje nesankcionuotoje šalyje. Jei daromos kopijos į skaitmenines laikmenas, jos turi būti laikomos nedegiame, rakinamame seife, esančiame atskiroje patalpoje.
185. Atsarginė kopija saugoma 2 (dvi) savaites, išskyrus atvejus susijusius su techninėmis aplinkybėmis. Pasibaigus saugojimo laikui, seniausia kopija ištrinama, vietoj jos įrašoma naujausia kopija.
186. “JIRA” registruojami visi atvejai, kai vykdomas duomenų atkūrimas iš atsarginių kopijų.
187. Informacinių išteklių atsarginis kopijavimas ir atstatymas vykdomas vadovaujantis Įmonės „Atsarginio kopijavimo ir atkūrimo iš atsarginių kopijų tvarka“.

XXIII. VEIKLOS TĘSTINUMO VALDYMAS

188. Įmonės veiklos tęstinumas valdomas vadovaujantis Įmonės vadovo patvirtintu veiklos tęstinumo valdymo planu. Veiklos tęstinumo planas rengiamas remiantis poveikio veiklai analize. Plane pateikiama ši informacija:
    188.1. Bendroji dalis – veiklos tęstinumo tikslai, plano apimtis, įgyvendinimo resursai ir atsakomybės;
    188.2. Poveikio veiklai analizė – kritinės Įmonės funkcijos ir jų praradimo poveikis, kritinių funkcijų valdytojai, kritines funkcijas užtikrinantys resursai (įskaitant informacinius resursus), reikalavimai funkcijų atkūrimo laikui, apimtims ir resursams, kritinėms funkcijoms ir resursams kylančios rizikos ir grėsmių scenarijai;
    188.3. Veiklos tęstinumo strategijos – reagavimo, krizinių ir nenumatytų situacijų valdymo/komunikavimo struktūros, kritinių funkcijų tęstinumo ir atkūrimo procedūros ir resursai;
    188.4. Tęstinumo plano palaikymas – plano išbandymo, komunikavimo ir atnaujinimo nuostatos, personalo mokymai.
189. Įmonės informacinių sistemų veiklos tęstinumas valdomas vadovaujantis IT skyriaus vadovo patvirtintu „Veiklos tęstinumo valdymo planu“. Plane pateikiama ši informacija:
    189.1. Bendroji dalis – informacinių sistemų aprašymas, plano tikslai ir apimtis, personalo vaidmenys ir atsakomybės;
    189.2. Plano aktyvavimas ir informavimas - aktyvavimo kriterijai ir atsakomybės, informavimo / komunikacijos priemonės ir procedūros, poveikio masto įvertinimo procedūros;
    189.3. Atkūrimas - atkūrimo strategijos, informacinių sistemų komponentų atkūrimo eiliškumas, detalios atkūrimo procedūros, susijusių šalių informavimo procedūros,

atkūrimo patvirtinimo procedūros, plano atšaukimo procedūros;

189.4. Plano išbandymo reikalavimai;

189.5. Priedai - visa sėkmingam atkūrimui būtina informacija (kontaktinė personalo informacija ir paslaugų teikėjų informacija, programinės ir aparatinės įrangos sąrašai ir kt.).

190. Už „Veiklos tęstinumo valdymo plano“ atnaujinimą, testavimo inicijavimą, testavimo rezultatų dokumentavimą bei korekcinių priemonių nustatymą atsakingas Kibernetinio saugumo vadovas.

191. Detalesnė veiklos tęstinumo valdymo procedūra pateikiama „Veiklos tęstinumo valdymo plane“.

XXIV. RIZIKŲ VERTINIMAS

192. Rizikos, kylančios Įmonės valdomiems informaciniams ištekliams vertinamos periodiškai, bet ne rečiau kaip kartą per metus, arba reikšmingai pasikeitus Įmonės veiklos pobūdžiui, informacinių išteklių valdymo priemonėms.

193. Rizikų vertinimas atliekamas vertinant rizikos veiksnius, galinčius turėti įtakos informacinių išteklių saugumui, jų galimą žalą, pasireiškimo tikimybę ir pobūdį, galimus rizikos valdymo būdus, rizikos priimtinumo kriterijus.

194. Svarbiausi rizikos veiksniai:

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

196. subjektyvūs tyčiniai (nesankcionuotas informacinių sistemų naudojimas informacijai gauti, informacijos pakeitimas ar sunaikinimas, duomenų perdavimo tinklais sutrikdymas, saugos pažeidimai, vagystės ir kita);

197. Rizikų vertinimo rezultatai išdėstomi rizikų vertinimo ataskaitoje, kuri teikiama Įmonės Vadovui ir apima:

197.1. rizikos valdymo planą tais atvejais, kai rizikos vertinimo metu yra nustatoma šalinamų trūkumų;

197.2. tinklų ir informacinių sistemų turto identifikavimą, poveikio vertinimą, grėsmių ir spragų vertinimo informaciją bei rizikos apskaičiavimo rezultatus pagal Įmonės nustatytus kriterijus, taip pat rizikos valdymą.

198. Atsižvelgdamas į rizikų vertinimo ataskaitą, Įmonės vadovas prireikus tvirtina rizikų valdymo priemonių planą, kuriame, be kita ko, numatomas techninių, administracinių ir kitų išteklių poreikis rizikų valdymo priemonėms įgyvendinti.

199. Remiantis periodiniu rizikos vertinimu nustatomos priemonės, kurios sumažina grėsmių poveikį mažinant pažeidžiamumų kiekį ir apimtį. Taip pat nustatomi reikalingi ištekliai, asmenys, atsakingi už šių priemonių įgyvendinimą bei įgyvendinimo terminus.

200. Įmonės vadovo paskirtas asmuo, atsakingas už rizikos vertinimo procesą, teikia rizikos vertinimo ataskaitos ir rizikos valdymo plano patvirtinimo duomenis, nurodydamas patvirtinimo datą ir registracijos numerį bei rizikos vertinimo metu nustatytus apibendrintus rezultatus: identifikuotas grėsmes, jų tikimybę ir poveikį veiklai, rizikos lygius ir valdymo priemones, į KSIS ne vėliau kaip per 5 darbo dienas nuo šių dokumentų patvirtinimo.

201. Įmonės vadovo arba jo įgalioto asmens patvirtintos rizikos vertinimo ataskaitos ir rizikos valdymo planai turi būti saugomi ne mažiau kaip 3 metus.

202. Rizikos vertinimo ir valdymo procedūra dokumentuota „Rizikos valdymo politikoje“.

203. Informacinių išteklių saugumo būklė gerinama techninėmis, programinėmis, organizacinėmis ir kitomis saugos priemonėmis, kurios pasirenkamos atsižvelgiant į Įmonės turimus išteklius, vadovaujantis šiais principais:
    203.1. likutinė rizika turi būti sumažinta iki priimtino lygio;
    203.2. informacinių išteklių saugumo priemonių diegimo kaina turi būti proporcinga saugomų informacinių išteklių vertei;
    203.3. atsižvelgiant į priemonių efektyvumą ir taikymo tikslingumą, turi būti įdiegtos prevencinės, aptikimo ir korekcinės saugos priemonės.

XXV. PAŽEIDŽIAMUMŲ VALDYMAS

204. Siekiant sumažinti saugos incidentų tikimybę, Įmonėje vykdomas informacinių sistemų techninių pažeidžiamumų identifikavimas ir šalinimas pagal Įmonėje patvirtintą „Pažeidžiamumų valdymo tvarką“.
205. Pažeidžiamumai (arba spragos) nustatomi pagal iš anksto parengtą pažeidžiamumų (arba spragų) nustatymo planą, kuriame:
    205.1. Apibrėžta, kokios sistemos, tinklai, įrenginiai ir aplikacijos bus įtraukti į spragų nustatymo procesą;
    205.2. Aprašyta, kokie metodai, įrankiai ir (ar) programinė įranga bus naudojami pažeidžiamumams nustatyti;
    205.3. Nurodyta, kas atsakingas už spragų nustatymo plano vykdymą;
    205.4. Spragų vertinimas, klasifikavimas ir prioritetų nustatymas;
    205.5. Veiksmų planas pažeidžiamumo spragoms šalinti;
    205.6. Pažeidžiamumo vertinimo periodiškumas;
    205.7. Spragų nustatymo ir trūkumų šalinimo ataskaita.
206. Visos darbo vietos, tarnybinės stotys, tinklo įrenginiai ir kt. turi įdiegtas saugumo pataisas tam, kad apsaugoti Informacines sistemas nuo pažeidžiamumų.
207. Įmonėje naudojamos pažeidžiamumų stebėjimo ir valdymo priemonės, kurių pagalba reguliariai tikrinama techninės ir programinės įrangos būklė.
208. Pažeidžiamumai turi būti vertinami reguliariai, o taip pat prieš paleidžiant naują sistemą ar atlikus esminius tinklo pokyčius, yra atliekamas vidinis ir išorinis sistemų skanavimas, siekiant nustatyti pažeidžiamumus Įmonės valdomoje įrangoje.
209. Kritinėms informacinėms sistemoms ir jų komponentams, kurie pasiekiami iš vidinio tinklo, vykdomas reguliarus, ne rečiau kaip kartą per metus, automatizuotas vidinis pažeidžiamumų skenavimas.
210. Kritinėms informacinėms sistemoms ir jų komponentams, kurie pasiekiami iš interneto, vykdomas reguliarus, ne rečiau kaip kartą per pusmetį, pažeidžiamumų skenavimas.
211. Visi aktyviniai tinklo įrenginiai turintys IP adresus tikrinami nuo pažeidžiamumų.
212. Kritiniai pažeidžiamumai privalo būti pašalinti ne ilgiau kaip per 14 dienų nuo pažeidžiamumo identifikavimo dienos.
213. Svarbūs pažeidžiamumai privalo būti pašalinti ne ilgiau kaip per 30 dienų nuo pažeidžiamumo identifikavimo dienos.
214. Kiti pažeidžiamumai privalo būti pašalinti ne ilgiau kaip per 60 dienų nuo pažeidžiamumo identifikavimo dienos.
215. Už pažeidžiamumų vertinimą atsakingas Kibernetinio saugumo vadovas.
216. Visų pažeidžiamumų tvarkymas turi būti suderintas su Įmonės numatytomis „IT keitimų valdymo aprašas“ ir „Kibernetinio saugumo incidentų valdymo plano“ nuostatomis.

XXVI. SANTYKIAI SU IŠORINĖMIS ŠALIMIS

217. Įmonės darbuotojai laikosi nustatytų „Paslaugų teikėjų ir tiekimo grandinės valdymo reikalavimų“, paslaugų, darbų ar įrangos pirkimams, susijusiems su tinklų ir informacinių sistemų projektavimu, kūrimu, diegimu, naudojimu, priežiūra, modernizavimu ir (ar) kibernetinio saugumo užtikrinimu, siekiant mažinti galimas kilti rizikas tinklų ir informacinėms sistemoms.
218. Tinklų ir informacinių sistemų tiekėjų atrankos procese įtraukti kibernetinės saugos kriterijai:
    218.1. Išorinės šalies atitiktis nustatytiems kibernetinio saugumo reikalavimams;
    218.2. kokybės reikalavimus tinklų ir informacinių sistemų produktams, paslaugoms;
    218.3. prieigų valdymas, įskaitant prieigų laikotarpio ribojimą;
    218.4. išorinės šalies personalui reikalingus įgūdžius ir (ar) mokymus, ir (ar) sertifikatus, ir (ar) kvalifikaciją, kiek tai susiję su teikiamomis paslaugomis;
    218.5. reikalavimus, keliamus Išorinės šalies patalpoms, įrangai, tinklų ir informacinių sistemų priežiūrai, informacijos perdavimui tinklais.
219. Teikdamas Išorinei šaliai prieigą prie Informacijos ar jos apdorojimo išteklių, Įmonės struktūrinis padalinys (skyrius), inicijuojantis sutarties su trečiąja šalimi sudarymą, įvertina galimas rizikas, atitiktį dėl saugumo reikalavimų. Jei nustačius, kad išorinė organizacija negali įvykdyti informacijos saugumo reikalavimų, prieiga neturėtų būti suteikta tol, kol neatitikimai nebus pašalinti;
220. Sutartyse su Išorine šalimi, kuriai yra suteikta prieiga prie Įmonės Informacijos ir (ar) Informacinių išteklių turi būti įtraukti Informacijos ir Asmens duomenų saugos reikalavimai, kokybės reikalavimai, prieigos valdymas, minimalūs kibernetinio saugumo reikalavimai tame tarpe ir nuostatos dėl konfidencialumo arba informacijos neatskleidimo reikalavimai. Taip pat numatoma Įmonės duomenų saugojimo terminų specifikacijos, tinklo saugumo ir saugumo stebėjimo procesai, duomenų centro vietos reikalavimai, ataskaitų teikimas, numatyti tiekėjo ir Įmonės teises ir pareigas numatytas Lietuvos Respublikos kibernetinio saugumo įstatyme. Jei duomenų perdavimo paslauga yra esminė Įmonės paslaugoms teikti, Įmonė su interneto teikėju turi būti sudaręs sutartį (-is), kurioje (-iose) turi būti numatyta:
    220.1. reagavimas į kibernetinius incidentus įprastomis darbo valandomis;
    220.2. nepertraukiamas paslaugos teikimas įprastomis darbo valandomis;
    220.3. paslaugos sutrikimų registravimas įprastomis darbo valandomis;
    220.4. apsaugos nuo tinklų ir informacinės sistemos trikdymo taikymas (DoS).
221. Išorinės šalies prieiga prie Įmonės informacijos ir (ar) Informacinių išteklių gali būti suteikiama tik tokios apimties, kiek tai būtina sutarčiai įgyvendinti ir nedelsiant panaikinama, pasibaigus sutartiniams santykiams.
222. Su Išorine šalimi turi būti sutarta, kokias priemones Išorinė šalis taikys Informacijos saugai užtikrinti (pvz., pasirašomas duomenų tvarkymo susitarimas), kaip bus valdomi incidentai, intelektinė nuosavybė ir autoriaus teisės, konfidencialumo ir duomenų neatskleidimo įsipareigojimai, subrangovai, teisė audituoti, pažeidžiamumai, defektų ir konfliktų taisymas.
223. Pasirenkant Išorinę šalį - Duomenų tvarkytoją, kuris atliks Asmens duomenų tvarkymo veiksmus Įmonės vardu, pasitelkiamos tik tos Išorinės šalys, kurios suteikia pakankamai garantijų, patikimumo saugos priemonių apimtyje, detalūs reikalavimai apibrėžti dokumente „Asmens duomenų tvarkymo taisyklės “ .
224. Turi būti užtikrinta saugi tiekimo grandinė, Išorinės šalys ir visi subtiekėjai turi taip pat

laikytis Informacijos saugos reikalavimų.

225. Trečiojo asmens teikiamos paslaugos, jų kokybė, ataskaitos ir kiti dokumentai turi būti nuolat stebimi ir kontroliuojami, taip pat reguliariai atliekami auditai.
226. Įmonė turi būti sudariusi Išorės šalių sąrašą, jį tvarkyti ir pasikeitus sutartims peržiūrėti ir atnaujinti numatytu periodiškumu ir kai įvyksta reikšmingi pokyčiai arba reikšmingi incidentai, susiję su tiekėjais.
227. Įmonei naudojant debesijos pagrindu teikiamas paslaugas, joms taikomi prieigos, šifravimo ir kiti darbo principai yra tokie pat ir griežtesni, kaip ir dirbant su vidinėmis sistemomis.

XXVII. INFORMACIJOS SAUGUMO AUDITAS

228. Vidinis informacijos saugumo auditas turi būti atliekamas ne rečiau kaip kartą per metus.
229. Nepriklausomas Įmonės informacijos saugumo auditas turi būti atliekamas periodiškai, ne rečiau kaip kartą per 3 metus arba reikšmingai pasikeitus Įmonės veiklos pobūdžiui, informacinių išteklių valdymo priemonėms.
230. Audito vertinimo tvarka aprašyta „Kibernetinio saugumo reikalavimų veiksmingumo vertinimo tvarkoje“.

XXVIII. ATITIKTIS TEISINIAMS IR KITIEMS INFORMACIJOS SAUGUMO REIKALAVIMAMS

231. Įmonė turi imtis tinkamų priemonių užtikrinant naudojamos programinės įrangos teisėtumą (legalumą) ir apsaugant intelektinės autorių nuosavybės teises. Įmonėje turi būti parengti naudojamos programinės įrangos ir šios įrangos licencijų registrai.
232. Įmonės veiklos dokumentai (įskaitant elektroninius dokumentus) turi būti tinkamai valdomi ir apsaugoti nuo sugadinimo, praradimo, neteisėto naudojimo, pakeitimo ir naikinimo, laikantis Lietuvos Respublikos teisės aktų ir Įmonės veiklos reikalavimų.
233. Įmonėje turi būti parengta dokumentų valdymo tvarka, kurioje nurodomi pagrindiniai dokumentų (įskaitant elektroninius dokumentus) rengimo, tvarkymo, apskaitos, saugojimo ir naikinimo reikalavimai.
234. Įmonė privalo užtikrinti tinkamas darbuotojų ir klientų asmens duomenų apsaugos priemones nuo atsitiktinio ar neteisėto duomenų sunaikinimo, pakeitimo, atskleidimo ar neteisėto tvarkymo, laikantis Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymo, Lietuvos Respublikos elektroninių ryšių įstatymo ir kitų LR teisės aktų reikalavimų.
235. Įmonės visų lygių vadovai užtikrindami „Kibernetinio saugumo politikos“ ir kitų saugumo reikalavimų įgyvendinimą savo atsakomybės ribose privalo periodiškai vertinti šių reikalavimų vykdymą ir šalinti neatitikimus.
236. Atitikties vertinimo tvarka aprašyta „Kibernetinio saugumo reikalavimų veiksmingumo vertinimo tvarka“.

XXIX. BAIGIAMOSIOS NUOSTATOS

237. Už Politikos atnaujinimą ir peržiūrą, ne rečiau kaip vieną kartą per metus, yra atsakingas Kibernetinio saugumo vadovas. Peržiūros metu Kibernetinio saugumo vadovas įvertiną Politiką ir kitus susijusius dokumentus, jų veiksmingumą ir atitiktį Lietuvos Respublikos kibernetinį saugumą reglamentuojantiems įstatymams, o iškilus poreikiui, inicijuoja reikiamus pakeitimus. Neeilinė peržiūra atliekama, įvykus pokyčiams, galintiems turėti įtakos

informacijos saugumui ir jo valdymui.

238. Politika yra sudėtinė Įmonės teisės aktų, reglamentuojančių kibernetinės saugos reikalavimus Įmonėje, dalis.

239. Įmonė rengia Politikos įgyvendinimo tvarkų aprašus, taisykles, procesus ar kitus su Informacijos sauga susijusius Įmonės teisės aktus, vadovaujantis šios Politikos nuostatomis ir laikantis teisės aktų.

240. Įmonė pateikia ir (ar) atnaujina Politikos dokumento (-ų) patvirtinimo duomenis, nurodydami dokumento pavadinimą, patvirtinimo datą ir registracijos numerį, NKSC į KSIS ne vėliau kaip per 5 darbo dienas nuo šio dokumento (-ų) patvirtinimo ir (ar) pakeitimo dienos, kai subjektas yra įtraukiamas į kibernetinio saugumo subjektų registrą.

241. Politika taikoma visiems Įmonės darbuotojams.

242. Visi Įmonės darbuotojai turi būti pasirašytinai susipažinę ar elektroninių priemonių pagalba patvirtinę susipažinimą su Politika.

243. Politika yra skelbiama viešai VASA interneto svetainėje, skiltyje „Apie įmonę“ -> „Korporatyvinė informacija“ -> „Svarbūs dokumentai“.

244. Politiką ir jos pakeitimus tvirtina Įmonės valdyba.

XXX. SUSIJĘ DOKUMENTAI

245. Politiką papildo šie dokumentai:

Susiję dokumentai
Prieigos prie informacinių sistemų ir jose saugomų duomenų tvarkos aprašas
Techninės ir programinės įrangos naudojimosi taisyklės
IT keitimų valdymo tvarkos aprašas
Atsarginio kopijavimo ir atkūrimo iš atsarginių kopijų tvarkos aprašas
Duomenų naikinimo ir šalinimo tvarkos aprašas
Veiklos tęstinumo valdymo plano aprašas
Kibernetinio saugumo incidentų valdymo planas
Nuotolinio darbo tvarka
Rizikų valdymo politika
Informacijos klasifikavimo reikalavimai
Paslaugų teikėjų ir tiekimo grandinės valdymo reikalavimai
Kriptografijos ir šifravimo naudojimo tvarka
Pažeidžiamumų valdymo tvarka
Kelių veiksnių tapatumo nustatymo sprendimų, saugių balso, vaizdo ir teksto ryšių bei saugių avarinių sistemų subjekto viduje naudojimo tvarka
Kibernetinio saugumo reikalavimų veiksmingumo vertinimo tvarka
Tinklų ir informacinių sistemų fizinės prieigos reikalavimai
Saugumo operacijų centro valdymo tvarka