PATVIRTINTA
UAB „Biržų vandenys“ direktoriaus
2024 m. gruodžio 2 d. Įsakymu Nr. V-76

UAB „BIRŽŲ VANDENYS“ INFORMACIJOS SAUGOS POLITIKA

I. BENDROSIOS NUOSTATOS

1.1. UAB „Biržų vandenys“, juridinio asmens kodas 154850665, adresas Rotušės g. 30, LT-41137, Biržai (toliau – Bendrovė, duomenų valdytojas) tvarko bendrovės darbuotojų ir kandidatų įsidarbinti bendrovėje asmens duomenis, vadovaudamasi Europos Parlamento Tarybos Reglamento (ES) 2016/679 (toliau – Reglamentas) nuostatomis ir kitais teisės aktais, reglamentuojančiais asmens duomenų apsaugą.

1.2. Šios Politikos tikslas – užtikrinti Bendrovės tvarkomų duomenų konfidencialumą, prieinamumą, vientisumą ir tinkamą kompiuterizuotų darbo vietų bei kompiuterių tinklo įrangos funkcionavimą.

1.3. Šioje Politikoje vartojamos sąvokos:

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

1.3.2. *Elektroninės informacijos sauga* – elektroninės informacijos konfidencialumo, vientisumo ir prieinamumo užtikrinimas.

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

1.3.4. *Bendrovės informacinė sistema (toliau sutrumpintai – IS)* - informacinių technologijų pagrindu veikianti sistema, užtikrinanti kompiuterizuotą duomenų, dokumentų ir kitos informacijos kūrimą, tvarkymą ir saugojimą bendrovės veikloje. Informacinę sistemą sudaro techninė įranga (tarnybinės stotys, darbo vietų kompiuteriai, duomenų saugyklos, kompiuterių tinklo ir elektroninio ryšio priemonės, duomenų apsaugos priemonės), programinė įranga (operacinės sistemos, pagalbinės programos, standartinė taikomoji programinė įranga ir specialioji taikomoji programinė įranga) ir kita kompiuterizuotai tvarkoma informacija

1.3.5. *IS administratorius* – Bendrovės įgaliotas darbuotojas/įmonė, prižiūrintis informacines sistemas Bendrovėje, Bendrovės naudojamos techninės ir programinės įrangos infrastuktūrą bei atsakingas už elektroninės informacijos saugos užtikrinimą bendrovėje. IS administratorius Bendrovėje atlieka ir saugos įgaliotinio funkcijas.

1.3.6. *IS naudotojas* – Bendrovės darbuotojas, ar kitas asmuo, pagal kompetenciją naudojantis ir (ar) tvarkantis elektroninę informaciją Bendrovės IS.

1.3.7. *Konfidencialumas* – elektroninės informacijos savybė – su IS tvarkoma elektronine informacija gali susipažinti tik tą daryti įgalioti asmenys.

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

1.3.9. *Vientisumas* – elektroninės informacijos savybė – elektroninė informacija nebuvo atsitiktinai ar neteisėtai pakeista ar sunaikinta.

1.4. Bendrovės informacijos saugos užtikrinimo prioritetinės kryptys ir tikslai:

1.4.1. organizacinių, techninių, programinių, teisinių ir kitų priemonių, skirtų IS duomenų saugai užtikrinti, įgyvendinimas ir kontrolė;

1.4.2. elektroninės informacijos konfidencialumas;

1.4.3. elektroninės informacijos prieinamumas;

1.4.4. elektroninės informacijos vientisumas;

1.4.5. IS veiklos tęstinumo užtikrinimas;

1.4.6. asmens duomenų apsauga;

1.4.7. IS naudotojų mokymas.

1.5. IS valdytoja yra Bendrovė.

1.6. IS administratorius atlieka šias funkcijas:

1.6.1. koordinuoja ir prižiūri IS saugos politikos įgyvendinimą;

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

1.6.3. teikia IS naudotojams privalomus vykdyti nurodymus ir pavedimus, susijusius su šios politikos įgyvendinimu;

1.6.4. reikalui esant organizuoja IS rizikos vertinimus;

1.6.5. periodiškai inicijuoja IS naudotojų supažindinimą informacijos saugos klausimais, informuoja juos apie informacijos saugos problematiką, siųsdamas priminimus ir konsultuodamas elektroniniu paštu, organizuodamas teminius seminarus ir mokymus, rengdamas ir pateikdamas atmintines naujai priimtiems darbuotojams;

1.6.6. supažindina IS naudotojus su informacinio saugumo politika Bendrovėje;

1.6.7. atsako už IS duomenų saugos politikos įgyvendinimo organizavimą;

1.6.8. atsako už IS naudotojų registravimą, prieigos teisių nustatymą, tinkamą infrastruktūros funkcionavimą;

1.6.9. atlieka funkcijas, susijusias su tarnybinių stočių administravimu, informacinės sistemos komponentų (kompiuterių, operacinių sistemų, duomenų bazių valdymo sistemų, taikomųjų programų sistemų, ugniasienių, įsilaužimų aptikimo sistemų, elektroninės informacijos perdavimo tinklais, bylų serveriais ir kt.) administravimu, šių informacinės sistemos komponentų sąranka, informacinių sistemų pažeidžiamų vietų nustatymu, saugumo reikalavimų atitikties nustatymu ir stebėsena, reagavimu į elektroninės informacijos saugos incidentus, taip pat administruoja pašto ir paieškos sistemas;

1.6.10. registruoja saugos įvykius, teikia pasiūlymus dėl įvykį sukėlusių priežasčių pašalinimo;

1.6.11. parengia ir diegia saugos priemones;

1.6.12. atlieka kitas reikalingas šiai politika įgyvendinti funkcijas.

1.7. Ši Politika privaloma visiems Bendrovės darbuotojams.

II. ELEKTRONINĖS INFORMACIJOS SAUGOS VALDYMAS

2.1. Bendrovės darbuotojai, pastebėję pažeidimų, nusikalstamos veikos požymių, neveikiančias arba netinkamai veikiančias saugos užtikrinimo priemones, privalo nedelsdami pranešti apie tai IS administratoriui.

2.2. Įtaręs neteisėtą veiką, pažeidžiančią ar neišvengiamai pažeisiančią informacinės sistemos saugą, IS administratorius apie tai turi pranešti Bendrovės vadovui ir kompetentingoms institucijoms, tiriančioms elektroninių ryšių tinklų, informacijos saugumo incidentus, neteisėtas veikas, susijusias su elektroninės informacijos saugos incidentais.

2.3. Informacijos saugos priemonės parenkamos atlikus informacinių technologijų saugos atitikties vertinimą. Pagrindiniai elektroninės informacijos saugos priemonių parinkimo principai yra šie:

2.3.1. liekamoji rizika turi būti sumažinta iki priimtino lygio;

2.3.2. elektroninės informacijos saugos priemonės diegimo kaina turi būti adekvati saugomos elektroninės informacijos vertei;

2.3.3. kur galima, turi būti įdiegtos prevencinės, grėsmes aptinkančios ir jas mažinančios elektroninės informacijos saugos priemonės.

2.4. Elektroninės informacijos saugos priemonės yra parenkamos atsižvelgiant į poreikį ir Bendrovės turimus resursus.

III. ORGANIZACINIAI IR TECHNINIAI REIKALAVIMAI

3.1. Bendrovė darbuotojams prieigos prie IS suteikimo tvarka nustatoma šios Politikos Priede Nr. 1 - Naudotojų administravimo taisyklėse – nustatyta tvarka.

3.2. Prieiga darbuotojams suteikiama tik prie tų išteklių, kurie yra būtini tiesioginėms pareigoms atlikti.

3.3. Stacionarūs ir nešiojamieji IS naudotojų kompiuteriai turi būti naudojami tik su tiesioginių pareigų atlikimu susijusiai veiklai. Iš kompiuterių, kurie perduoti remontui ar techninei priežiūrai, turi būti pašalinta visa neviešintina elektroninė informacija.

3.4. Naudotojams draudžiama patiems diegti bet kokią programinę įrangą. Programinę įrangą, reikalingą naudotojo funkcijoms atlikti, diegia ir prižiūri IS administratorius.

3.5. IS naudotojų kompiuteriuose draudžiama naudoti programinę įrangą, nesusijusią su tiesiogine jų veikla ir funkcijomis.

3.6. IS kompiuteriuose turi būti naudojama tik legali programinė įranga.

3.7. Naudotojams gali būti suteikiama nuotolinio prisijungimo prie IS galimybė protokolu, skirtu duomenų šifravimui.

3.8. Saugos reikalavimai, taikomi jungiantis prie IS nuotoliniu būdu, turi būti ne mažesni nei jungiantis prie IS vidiniame Bendrovės tinkle.

3.9. Darbo vietų kompiuteriuose turi būti naudojama programinė įranga, skirta apsaugoti IS nuo kenksmingos programinės įrangos (virusų, programinės įrangos, skirtos šnipinėti, nepageidaujamo elektroninio pašto ir pan.) (toliau – antivirusinė programinė įranga). Antivirusinė programinė įranga turi būti atnaujinama kartą per parą.

3.10. IS funkcionuoti būtina programinė įranga (operacinės sistemos, aplikacijos, interneto naršyklės, interneto naršyklių priedai ir kt.) turi būti konfigūruojama laikantis programinės įrangos gamintojų saugaus konfigūravimo rekomendacijų. Už tarnybinių stočių programinės įrangos kontrolę atsako IS administratorius.

3.11. IS duomenys perduodami automatiniu būdu, naudojant TCP/IP protokolą

3.12. Prieiga prie duomenų ribojama pagal IP adresą.
3.13. IS administratorius tvarko ir ne rečiau kaip kartą per 3 mėnesius atnaujina Bendrovės techninių išteklių ir programinės įrangos registrą.
3.14. Detali informacija apie organizacinius ir techninius reikalavimus pateikiama Priede Nr. 2 - Saugaus elektroninės informacijos tvarkymo taisyklėse.
3.15. Įvykus elektroninės informacijos saugos incidentui:
3.15.1. Incidentą pastebėjęs bendrovės darbuotojas nedelsdamas privalo informuoti IS Administratorių;
3.15.2. IS Administratorius nedelsdamas informuoja apie situaciją Bendrovės vadovą;
3.15.3. Derindamas veiksmus su Bendrovės vadovu, Administratorius:
3.15.4. Fiksuoja informaciją elektroninės informacijos saugos incidentų registravimo žurnale, reikalui esant – praneša apie incidentą įgaliotoms valstybės institucijoms,
3.15.5. pagal galimybes atkuria tarnybinių stočių, kompiuterių ir kitą Bendrovės veiklą, duomenis, techninės, sisteminės ir taikomosios programinės įrangos funkcionavimą;
3.15.6. organizuoja žalos Informacinės sistemos duomenims, techninei bei programinei įrangai vertinimą,
3.15.7. koordinuoja Informacinės sistemos veiklai atkurti reikalingos techninės, sisteminės ir taikomosios programinės įrangos įsigijimą;
3.15.8. jei incidentas susijęs su Bendrovės atliekamomis asmens duomenų tvarkymo operacijomis - veikia pagal Bendrovės Asmens duomenų saugumo pažeidimų nustatymo, tyrimo, pranešimo apie juos ir dokumentavimo taisykles.

IV. REIKALAVIMAI PERSONALUI

4.1. IS Naudotojai privalo rūpintis tvarkomos elektroninės informacijos sauga.
4.2. IS Naudotojai turi būti susipažinę su šia Politika.
4.3. IS administratorius privalo išmanyti informacijos saugos principus, mokėti užtikrinti jų saugą, administruoti ir prižiūrėti duomenų bazes, sugebėti užtikrinti IS techninės ir programinės įrangos nepertraukiamą funkcionavimą, stebėti techninės ir programinės įrangos veikimą, atlikti techninės ir programinės įrangos profilaktinę priežiūrą, sutrikimų diagnostiką ir šalinimą, išmanyti elektroninės informacijos saugos užtikrinimo principus, turi būti susipažinęs su IS duomenų saugos politiką įgyvendinančiais dokumentais, darbo saugos taisyklėmis.
4.4. IS naudotojai privalo turėti pagrindinius darbo su kompiuteriu įgūdžius, mokėti tvarkyti duomenis IS nuostatų nustatyta tvarka ir būti susipažinę su IS duomenų saugos politiką įgyvendinančiais dokumentais ir kitais teisės aktais, įgyvendinančiais duomenų saugos politiką, su atsakomybe už IS duomenų saugos politikos pažeidimą.
4.5. Naudotojams turi būti reguliariai rengiami elektroninės informacijos saugos mokymai, įvairiais būdais primenama apie elektroninės saugos problematiką (pvz., priminimai elektroniniu paštu, teminių seminarų rengimas, atmintinės). Saugos mokymai organizuojami ne rečiau kaip kartą per 1 metus. Mokymai, susiję su asmens duomenų apsauga, organizuojami ne rečiau kaip kartą per 1 metus. Mokymus organizuoja ir jų efektyvumą vertina IS administratorius.
4.6. Už saugos dokumentuose nustatytų reikalavimų nesilaikymą yra atsakingi IS naudotojai.

V. INFORMACINĖS SISTEMOS NAUDOTOJŲ SUPAŽINDINIMO SU SAUGOS DOKUMENTAIS PRINCIPAI

5.1. Naudotojo supažindinimas su šia Politika turi būti vykdomas šiais atvejais:

5.1.1. prieš suteikiant naudotojui prieigą prie IS;

5.1.2. pakeitus saugos politiką;

5.1.3. periodiškai, informacijos saugos mokymų metu, ne rečiau kaip kartą per 1 metus.

Priedas Nr.1
Prie UAB „UAB „Biržų vandenys“
Informacijos saugos politikos

UAB „BIRŽŲ VANDENYS“ INFORMACINĖS SAUGOS POLITIKA
NAUDOTOJŲ ADMINISTRAVIMO TAISYKLĖS

I. BENDROSIOS NUOSTATOS

1. Šios Naudotojų administravimo taisyklės (toliau – Taisyklės) nustato Bendrovės IS naudotojų įgaliojimus, teises ir pareigas.
2. Šios Taisyklės taikomos visiems Bendrovės IS naudotojams ir IS administratoriui.

II. INFORMACINĖS SISTEMOS NAUDOTOJŲ IR ADMINISTRATORIAUS ĮGALIOJIMAI, TEISĖS IR PAREIGOS

3. Naudotojai gali naudotis tik tomis IS dalimis ir jose apdorojamais duomenimis, prie kurių prieigą jiems suteikė IS administratorius.
4. Naudotojai privalo užtikrinti jų naudojamų duomenų konfidencialumą, vientisumą ir pasiekiamumą, vadovaudamiesi šiose taisyklėse apibrėžtais reikalavimais.
5. Naudotojai turi teisę reikalauti iš IS administratoriaus užtikrinti deramą jų naudojamų Informacinės sistemos ir joje apdorojamų duomenų apsaugos lygį, gauti jų pareigoms eiti būtiną informaciją apie taikomas apsaugos priemones ir rekomenduoti papildomas apsaugos priemones.
6. Naudotojų pareigos renkant, tvarkant, perduodant, saugant, naikinant ar kitaip naudojant elektroninę informaciją:

6.1. jungtis prie IS įvedant tik jiems asmeniškai suteiktus prisijungimo vardus ir slaptažodžius;
6.2. nesijungti prie IS naudojantis kitam darbuotojui suteiktais prisijungimo vardais ir slaptažodžiais;
6.3. nedelsiant pranešti IS administratoriui apie informacinės sistemos sutrikimus, neįprastą jų veikimą, esamus arba galimus elektroninės informacijos saugumo reikalavimų pažeidimus, kitų naudotojų nederamus veiksmus;
6.4. neatskleisti, nelaikyti matomoje vietoje suteiktų prisijungimo vardų ir slaptažodžių;
6.5. prisiimti atsakomybę už tinkamą elektroninės informacijos tvarkymo programinių priemonių naudojimą ir techninių priemonių saugojimą;
6.6. elektroninės informacijos tvarkymo programinę ir techninę įrangą naudoti tik darbinėms funkcijoms atlikti.
6.7. Naudotojai visiškai atsako už jų vardu atliktus veiksmus Bendrovės IS.
6.8. Naudotojams draudžiama naudotis Bendrovės IS asmeniniais tikslais.

7. IS administratorius turi teisę tikrinti naudotojų veiksmus IS ir imtis priemonių nutraukti neteisėtus veiksmus bei uždrausti prieigas iki visų aplinkybių išsiaiškinimo.
8. Iš darbo išėjusio Naudotojo slaptažodžiai ir kiti prisijungimo prie Bendrovės IS duomenys yra blokuojami. Slaptažodžiai ir prisijungimo informacija po užblokavimo saugomi tris mėnesius, po to sunaikinami.
9. Visiems Naudotojams yra sukuriamas asmeninis elektroninio pašto adresas. Papildomai gali būti sukurtas funkcinis elektroninio pašto adresas, priskirtas struktūriniam padaliniui ar darbuotojų grupei tam tikroms darbo funkcijoms vykdyti.
10. IS administratorius savo funkcijas atlieka naudodamas atskirą tam skirtą informacinės sistemos administratoriaus paskyrą, kuria naudojantis negalima atlikti informacinės sistemos naudotojo funkcijos.
11. Naudotojams negali būti suteikiamos informacinės sistemos administratoriaus teisės.

III. SAUGAUS DUOMENŲ TEIKIMO INFORMACINĖS SISTEMOS NAUDOTOJAMS KONTROLĖS TVARKA

12. Už prieigos prie informacinės sistemos suteikimą ir panaikinimą yra atsakingas administratorius. Nurodymus dėl prieigos suteikimo, keitimo ar naikinimo, Administratoriui teikia bendrovės vadovas.
13. Administratorius tvarko asmenų (naudotojų), kuriems suteiktos, pakeistos ar panaikintos teisės prisijungti prie Bendrovės IS, sąrašą.
14. Naudotojų tapatybė informacinėje sistemoje yra nustatoma pagal unikalų vartotojo vardą (kuris negali sutapti su naudotojo asmens kodu) ir slaptažodį.
15. Visiems slaptažodžiams yra keliami šie reikalavimai:
15.1. slaptažodį turi sudaryti ne mažiau kaip 8 simboliai;
15.2. slaptažodis turi būti sudarytas iš raidžių, skaičių ir specialiųjų simbolių;
15.3. slaptažodžiams sudaryti neturi būti naudojama asmeninio pobūdžio informacija;
15.4. draudžiama slaptažodžius atskleisti tretiesiems asmenims;
15.5. didžiausias leistinas mėginimų įvesti teisingą slaptažodį skaičius - 5 kartai; slaptažodį, neteisingai įvedus didžiausią leistiną skaičių, informacinė sistema turi užsirakinti ir neleisti informacinės sistemos naudotojui identifikuotis informacinės sistemos laiko tarpą, kuris turi būti ne trumpesnis nei 15 minučių;
15.6. slaptažodžiai negali būti saugomi ar perduodami atviru tekstu ar užšifruojami nepatikimais algoritmais;
15.7. slaptažodis turi būti keičiamas ne rečiau kaip kas 3 mėnesius;
15.8. keičiant slaptažodį informacinė sistema neturi leisti sudaryti slaptažodžio iš buvusių 6 paskutinių slaptažodžių;
15.9. pirmojo prisijungimo prie informacinės sistemos metu iš informacinės sistemos naudotojo turi būti reikalaujama, kad jis pakeistų slaptažodį.
16. Bendrovės IS administratoriaus slaptažodis gali būti žinomas tik IS administratoriui.
17. Slaptažodžiai saugomi naudojant kodavimo formą (*hash-form*).
18. Draudžiama naudoti programinės įrangos gamintojų nustatytus slaptažodžius – jie turi būti pakeisti į šių Taisyklių reikalavimus atitinkančius slaptažodžius.
19. Administratorius apriboja Naudotojui prieigos teises, jeigu kyla įtarimų, kad naudotojas piktnaudžiauja suteiktomis prieigos teisėmis ir gali pažeisti informacinės sistemos arba joje apdorojamų duomenų saugumą. Reikalui esant, Administratorius kreipiasi į Bendrovės vadovą, kad gautų leidimą panaikinti naudotojo prieigos teisę.
20. Naudotojui teisė dirbti su konkrečia elektronine informacija sustabdoma, kai darbuotojas nušalinamas nuo darbo ar pasibaigus darbo santykiams. Naudotojo teisės naudotis Bendrovės IS taip pat naikinamos raštu nurodžius Bendrovės vadovui.
21. Administratorius periodiškai tikrina, ar nėra nepatvirtintų/neaktyvių administratoriaus ar/ir naudotojų paskyrų.
22. Nereikalingos ar nenaudojamos naudotojų ir administratoriaus paskyros blokuojamos nedelsiant ir ištrinamos praėjus nustatytam saugojimo terminui.
23. Naudotojams gali būti suteikiama nuotolinio prisijungimo prie IS galimybė protokolu, skirtu duomenų šifravimui.

Priedas Nr.2
Prie UAB „UAB „Biržų vandenys“
Informacijos saugos politikos

UAB „BIRŽŲ VANDENYS“ INFORMACIJOS SAUGUMO POLITIKOS
SAUGAUS ELEKTONINĖS INFORMACIJOS TVARKYMO TAISYKLĖS

I. BENDROSIOS NUOSTATOS

1. Šios Taisyklės nustato tvarką, kuria vadovaujantis saugiai tvarkoma elektroninė informacija Bendrovės IS.
2. Taisyklės yra privalomos visiems Bendrovės darbuotojams.
3. Už Taisyklių įgyvendinimą ir jų laikymosi kontrolę atsakingas Bendrovės IS administratorius.
4. Bendrovės IS saugomą bei apdorojamą elektroninę informaciją sudaro visi skaitmeniniai dokumentai, informacija esanti Bendrovės kompiuteriuose ir serveriuose.
5. Už Bendrovės elektroninės informacijos tvarkymą atsakingi Bendrovės IS naudotojai, dirbantys su atitinkama informacija. Teisės jiems suteikiamos ir prižiūrimos IS administratoriaus Naudotojų administravimo taisyklėse nustatyta tvarka.

II. TECHNINĖS IR KITOS SAUGOS PRIEMONĖS

6. Bendrovės techninės įrangos saugos priemonės:
6.1. Bendrovės IS įdiegta patikima duomenų saugykla ir rezervinio kopijavimo įranga;
6.2. visa Bendrovės IS techninė įranga privalo turėti šios įrangos gamintojų garantinį arba pratęstą pogarantinį aptarnavimą;
6.3. Bendrovės kompiuterių ir kitos techninės įrangos keitimas gali būti atliekamas tik gavus IS administratoriaus leidimą;
6.4. Bendrovės IS tarnybinių stočių įranga turi perspėti IS administratorių, kai tarnybinėse stotyse sumažėja iki nustatytos pavojingos ribos laisvos operatyviosios atminties ar vietos diske (diskuose) ar duomenų saugykloje, ilgą laiką stipriai apkraunamas centrinis procesorius ir/ar tinklo sąsaja.
7. Bendrovės IS programinės įrangos saugos priemonės:
7.1. Bendrovėje naudojama tik legali ir įteisinta sisteminė ir taikomoji programinė įranga;
7.2. IS Naudotojų kompiuterinėje įrangoje turi būti naudojama tik legali ir tik darbo funkcijoms atlikti reikalinga programinė įranga;
7.3. Bendrovės IS administratorius parengia, su Bendrovės vadovu suderina ir ne rečiau kaip kartą per metus peržiūri bei prireikus atnaujina leistinos programinės įrangos sąrašą;
7.4. Bendrovės IS naudojama nuolat automatiškai atnaujinama antivirusinė programinė įranga;
7.5. Bendrovės IS naudotojui baigus darbą imamasi priemonių, kad su Bendrovės IS saugoma elektronine informacija negalėtų susipažinti pašaliniai asmenys:
7.5.1. atsijungiama nuo Bendrovės informacinės sistemos;
7.5.2. įjungiama ekrano užsklanda su slaptažodžiu;
7.5.3. dokumentai ar jų kopijos darbo vietoje turi būti padedami į pašaliniams asmenims neprieinamą vietą;
7.6. Bendrovės IS naudotojui neatliekant jokių veiksmų 15 minučių, IS turi taip užsirakinti, kad toliau ja naudotis galima būtų tik pakartojus tapatybės nustatymo ir autentiškumo patvirtinimo veiksmus;
7.7. Bendrovės IS naudojamos centralizuotai valdomos ir atnaujinamos kenksmingosios programinės įrangos aptikimo, stebėjimo realiu laiku priemonės; šios priemonės automatiškai turi informuoti IS administratorių apie galimus pažeidimus arba neatitikimus.

8. Elektroninės informacijos perdavimo tinklais saugumo užtikrinimo priemonės:

8.1. Bendrovės IS elektroninės informacijos perdavimo tinklas atskirtas nuo viešųjų ryšių tinklų naudojant ugniasienę; ugniasienės įvykių žurnalai (angl. Logs) reguliariai analizuojami, o ugniasienės saugumo taisyklės periodiškai peržiūrimos ir atnaujinamos;

8.2. Bendrovės IS programinė įranga turi turėti apsaugą nuo pagrindinių per tinklą vykdomų atakų;

8.3. Bendrovės IS tinklo perimetro apsaugai turi būti naudojami filtrai, apsaugantys elektroniniame pašte ir viešame ryšių tinkle naršančių IS naudotojų kompiuterinę įrangą nuo kenksmingo kodo.

9. Patalpų ir aplinkos saugumo užtikrinimo priemonės:

9.1. Bendrovės IS infrastruktūra bei ją palaikančios sistemos turi būti fiziškai apsaugotos nuo nesankcionuotos prieigos, vagystės, sugadinimo ar sunaikinimo;

9.2. Bendrovės IS tarnybinių stočių patalpose turi būti įrengti gaisro ir įsilaužimo davikliai, prijungti prie pastato signalizacijos ir (arba) apsaugos tarnybos stebėjimo pulto;

9.3. Ne Bendrovės darbuotojai į IS infrastruktūros patalpą gali patekti ir dirbti jame tik lydimi Bendrovės IT administratoriaus arba kito bendrovės darbuotojo;

9.4. IS kompiuterinė įranga turi turėti įtampos filtrą ir rezervinį maitinimo šaltinį, užtikrinantį informacinės sistemos pagrindinės kompiuterinės įrangos veikimą.

III. SAUGUS ELEKTRONINĖS INFORMACIJOS TVARKYMAS

10. IS naudotojai identifikuojami pagal informacinės sistemos naudotojų vardus ir slaptažodžius, kurių kontrolę atlieka kompiuterių ir serverių operacinės sistemos.

11. Bendrovės IS duomenų keitimą, atnaujinimą, įvedimą ir naikinimą gali atlikti tik tam turintys teisę autorizuoti naudotojai.

12. Bendrovės vykdomas programinės įrangos kūrimas atliekamas specialioje aplinkoje, neprijungtoje prie kitų IT sistemų, naudojamų tvarkant asmens duomenis. Testavimas nėra vykdomas su realiais asmens duomenimis arba, kai tai neįmanoma, nustatomos specialios apsaugos procedūros.

13. Siekiant nustatyti neteisėtus veiksmus su Bendrovės IS saugoma ir apdorojama elektronine informacija bei šios informacijos vientisumo pažeidimus, informacinėje sistemoje turi būti įrašomi ir saugomi duomenys apie informacinės sistemos tarnybinių stočių, informacinės sistemos taikomosios programinės įrangos įjungimą, išjungimą ar perkrovimą, sėkmingus ir nesėkmingus bandymus registruotis informacinės sistemos tarnybinėse stotyse, informacinės sistemos taikomojoje programinėje įrangoje, naudotojų ir/ar administratorių teisių naudotis sistemos ištekliais pakeitimus, įvisus informacinės sistemos naudotojų vykdomus veiksmus, kitus elektroninės informacijos saugai svarbius įvykius, įrašų kūrimą, keitimą ar trynimą, audito funkcijos įjungimą/išjungimą, nurodant informacinės sistemos naudotojo identifikatorių ir elektroninės informacijos saugai svarbaus įvykio ar vykdyto veiksmo datą ir laiką, įvykio duomenis bei rezultatą. Šie duomenys saugomi 6 mėnesius, ne toje pačioje informacinėje sistemoje, kurioje jie įrašomi, taip pat jie analizuojami ne rečiau kaip kartą per savaitę. Draudžiama šiuos duomenis trinti ar keisti, kol nesibaigęs jų saugojimo terminas.

14. Įsibrovimų aptikimas ir prevencija:

14.1. Bendrovės įdiegiamos ir veikia įsibrovimo aptikimo sistemos, kurios stebi Bendrovės IS įeinantį ir išeinantį duomenų srautą ir vidinį srautą tarp svarbiausių tinklo paslaugų;

14.2. Bendrovės pagrindinėse tarnybinėse stotyse veikia saugasienės, sukonfigūruotos blokuoti visą įeinantį ir išeinantį, išskyrus su Bendrovės IS funkcionalumu ir administravimu susijusį duomenų srautą;

15. Saugus naudojimasis belaidžiu tinklu ir mobiliaisiais įrenginiais:

15.1. Sprendimą dėl leidimo jungtis prie Bendrovės IS per belaidį tinklą priima Bendrovės IS administratorius. Tokio sprendimo nesant jungtis prie Bendrovės IS per belaidį tinklą nėra galimybės.

15.2. Jungtis prie Bendrovės IS per belaidį tinklą leidžiama tik Bendrovės darbuotojams, kuriems tai yra būtina tiesioginių jų funkcijų vykdymui.

15.3. Bendrovės IS administratorius apriboja galimybę jungtis prie Bendrovės IS per mobiliuosius įrenginius konkrečiam darbuotojui gavęs tiesioginį Bendrovės vadovo nurodymą tai atlikti arba jeigu kyla įtarimų, kad naudotojas piktnaudžiauja suteiktomis prieigos teisėmis ir gali pažeisti informacinės sistemos arba joje apdorojamų duomenų saugumą.

15.4. Belaidžių įrenginių kontrolė vykdoma tokiais būdais:

15.4.1. Tikrinami Bendrovės IS eksploatuojami belaidžiai įrenginiai, Bendrovės IS administratoriui pranešama apie neleistinus belaidžius įrenginius;

15.4.2. Leidžiama naudoti tik su Bendrovės IS administratoriumi suderintus belaidės prieigos taškus;

15.4.3. Prisijungiant prie belaidžio tinklo, turi būti taikomas ryšių ir informacinių sistemų naudotojų tapatumo patvirtinimo EAP (angl. Extensible Authentication Protocol) / TLS (angl. Transport Layer Security) protokolas;

15.4.4. Turi būti uždrausta belaidėje sąsajoje naudoti SNMP (angl. Simple Network Management Protocol) protokolą;

15.4.5. Turi būti uždrausti visi nebūtini valdymo protokolai;

15.4.6. Turi būti išjungti nenaudojami TCP (angl. Transmission Control Protocol) / UDP (angl. User Datagram Protocol) prievadai;

15.4.7. Turi būti uždraustas lygiarangis (angl. peer to peer) funkcionalumas, neleidžiantis belaidžiais įrenginiais palaikyti ryšį tarpusavyje;

15.4.8. Belaidis ryšys turi būti šifruojamas mažiausiai 128 bitų ilgio raktu.

16. Saugus naudojimasis mobiliaisiais įrenginiais:

16.1. Sprendimą dėl leidimo jungtis prie Bendrovės IS per mobiliuosius įrenginius priima Bendrovės IS administratorius. Tokio sprendimo nesant jungtis prie Bendrovės IS naudojant mobiliuosius įrenginius galimybė nesudaroma.

16.2. Jungtis prie Bendrovės IS per mobiliuosius įrenginius leidžiama tik Bendrovės darbuotojams, kuriems tai yra būtina tiesioginių jų funkcijų vykdymui. Bendrovės IS administratorius suteikia leidimą darbuotojui jungtis prie Bendrovės IS naudojant mobilųjį įrenginį tik gavęs Bendrovės vadovo nurodymą tai atlikti.

16.3. Bendrovės IS administratorius apriboja galimybę jungtis prie Bendrovės IS per mobiliuosius įrenginius konkrečiam darbuotojui gavęs tiesioginį Bendrovės vadovo nurodymą tai atlikti arba jeigu kyla įtarimų, kad naudotojas piktnaudžiauja suteiktomis prieigos teisėmis ir gali pažeisti informacinės sistemos arba joje apdorojamų duomenų saugumą.

16.4. Naudojant mobiliuosius įrenginius prisijungimui prie Bendrovės IS, turi būti:

16.4.1. laikomasi Bendrovės IS informacinės saugos politikos dokumentuose nurodytų atpažinties, tapatumo patvirtinimo ir naudojimosi Bendrovės IS saugumo ir kontrolės reikalavimų;

16.4.2. leidžiama naudoti tik mobiliuosius įrenginius, atitinkančius Bendrovės nustatytus saugumo reikalavimus;

16.4.3. Bendrovės IS administratorius turi turėti teises valdyti mobiliuosius įrenginius ir juose įdiegtą programinę įrangą.

16.5. Mobiliųjų įrenginių kontrolė vykdoma tokiais būdais:

16.5.1. Tikrinami Bendrovės IS naudojami mobilieji įrenginiai, Bendrovės IS administratoriui pranešama apie neleistinus mobiliuosius įrenginius;

16.5.2. Naudojamuose mobiliuosiuose įrenginiuose turi būti įdiegiamos operacinės sistemos ir kiti naudojamos programinės įrangos gamintojų rekomenduojami atnaujinimai;

16.5.3. Naudojamuose mobiliuosiuose įrenginiuose turi būti užtikrinta kompiuterinių laikmenų apsauga, t.y. užtikrinama, kad duomenys jose yra šifruojami.

17. Bendrovės interneto svetainių (toliau – Svetainė) saugos valdymo reikalavimai:

17.1. svetainė turi atitikti teisės aktuose numatytus saugumo reikalavimus;

17.2. svetainės užkardos turi būti sukonfigūruotos taip, kad prie svetainių turinio valdymo sistemų (toliau –

TVS) būtų galima jungtis tik iš vidinio informacinių sistemų tvarkytojo kompiuterinio tinklo arba nustatytų IP (angl. Internet Protocol) adresų;

17.3. turi būti pakeistos numatytos prisijungimo prie svetainių turinio valdymo sistemos (TVS) ir administravimo skydų (angl. Panel) nuorodos (angl. Default path) ir slaptažodžiai;

17.4. turi būti užtikrinama, kad prie svetainių TVS ir administravimo skydų būtų galima jungtis tik naudojantis šifruotu ryšiu;

18. Bendrovės IS duomenys kitoms IS teikiami ir/arba gaunami iš jų su šių IS valdytojais sudarytose duomenų teikimo sutartyse numatytais būdais, apimtimi, reguliarumu ir/arba terminais.

19. Bendrovės IS administratorius privalo naudoti visas reikiamas priemones, skirtas apsisaugojimui nuo neteisėto duomenų kopijavimo, keitimo, naikinimo ar perdavimo bei kilus įtarimui, kad su Bendrovės IS ir/arba jose saugomais ir apdorojamais duomenimis yra vykdoma neleidžiama veikla, apie tai informuoti Bendrovės vadovą, kuris tokiu atveju inicijuoja įvykio tyrimą.

20. Bendrovės IS techninės ir programinės įrangos priežiūra, keitimas ir atnaujinimas vykdomas IS administratoriaus, laikantis visų programinės ir techninės įrangos gamintojų rekomendacijų. Pakeitimų valdymas atliekamas per GitHUB. Bendrovės IS operatyviai ištestuojami ir įdiegiami gamintojų rekomenduojami atnaujinimai.

21. Nešiojamiesiems kompiuteriams, kuriems suteikiama prieiga prie Bendrovės IS, bei jų naudotojams, taikomi visi saugumo reikalavimai, numatyti stacionarioms kompiuterizuotoms darbo vietoms ir jų naudotojams. Informacija nešiojamųjų kompiuterių laikmenose šifruojama.

22. Atsarginių elektroninės informacijos kopijų darymo tvarka:

22.1. IS Administratorius yra atsakingas už reguliarų informacijos atsarginių kopijų darymą, užtikrinimą, kad jos būtų daromos numatytu laiku ir numatyta apimtimi, taip pat už reguliarų atsarginių kopijų atstatymo testavimą.

22.2. Atsarginės duomenų kopijos daromos automatiniu būdu: pridedamoji kopija daroma kasdien, o kas savaitę daroma pilna kopija;

22.3. Duomenų atkūrimas iš atsarginių kopijų testuojamas reguliariai, ne rečiau kaip kartą per 12 mėnesių;

22.4. Atsarginės kopijos turi būti saugomos numatytą laikotarpį (ne mažiau kaip 12 mėn.), vėliau jas sunaikinant arba užrašant naujesnėmis kopijomis;

22.5. Atsarginės kopijos saugomos šifruotu pavidalu;

22.6. Atsarginės kopijos saugomos atskirtose fizinėse vietose, patalpose, atitinkančiose šių Taisyklių reikalavimus;

22.7. Atsarginės kopijos apsaugomos nuo nesankcionuoto priėjimo, jų panaudojimo ar sunaikinimo;

22.8. Nebenaudojamos atsarginių kopijų laikmenos saugiai išvalomos ar sunaikinamos, be galimybės atkurti jose buvusius duomenis;

22.9. visi veiksmai su atsarginėmis kopijomis (darymo, testavimo, atstatymo, pervežimo, sunaikinimo) registruojami.

22.10. Administratorius privalo laikytis šiose Taisyklėse nustatytos atsarginių kopijų darymo tvarkos, tikrinti duomenų vientisumą, atliekant duomenų atstatymo testavimą; kartą per savaitę peržiūrėti atsarginių kopijų ir atstatymo įrašus.

IV. REIKALAVIMAI, KELIAMI BENDROVĖS IS FUNKCIONAVIMUI REIKALINGOMS PASLAUGOMS IR JŲ TEIKĖJAMS

23. Esant poreikiui, Bendrovės IS priežiūros paslaugų teikėjams suteikiami tokie prieigos prie IS lygiai ir sąlygos, kurie reikalingi ir pakankami priežiūros paslaugoms atlikti.

24. Reikalavimai Bendrovės IS priežiūros paslaugų teikėjams ir jų teikiamoms paslaugoms, bei kitoms paslaugoms ir jų teikėjams numatyti paslaugų teikimo sutartyse su teikėjais turi atitikti numatytuosius

dokumentuose reglamentuojančiuose tų paslaugų reikalavimus.

25. Reikalavimai interneto ryšio teikimo paslaugai nurodyti paslaugų teikimo sutartyje su interneto ryšio teikėju.
