PATVIRTINTA

UAB Ignalinos butų ūkio

direktoriaus

2021-12-17 įsakymu Nr. V-58

**UŽDAROSIOS AKCINĖS BENDROVĖS IGNALINOS BUTŲ ŪKIO**

**INFORMACIJOS saugojimo POLITIKA**

**Sąvokos**

**Šioje Uždarosios akcinės bendrovės Ignalinos butų ūkio informacijos saugumo politikoje (toliau – politika) vartotinos sąvokos turi būti suprantamos ir aiškinamos kaip nurodyta toliau:**

|  |  |
| --- | --- |
| **Bendrovė** | reiškia Uždarąją akcinę bendrovę Ignalinos butų ūkį, adresas -Turistų g. 9, 30105 Ignalina, juridinio asmens kodas 255512870, atsiskaitomoji sąskaita LT557300010002496525 AB „Swedbank“, įregistruotą Lietuvos Respublikos juridinių asmenų registre. |
| **BDAR** | reiškia 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentą (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas). |
| **UAB vadovas** | reiškia UAB Ignalinos butų ūkio vienasmenį valdymo organą |
| **Darbuotojas** | reiškia Uždarosios akcinės bendrovės darbuotoją |
| **Informacija** | reiškia tikslingi, prasmę turintys duomenys, kurie gali egzistuoti įvairiomis formomis (pvz. žodiniai, rašyti ranka, atspausdinti, sugeneruoti elektroniniu būdu šios Politikos kontekste yra laikomi tiek asmens duomenys, tiek bet kokia kita su Bendrovės veikla susijusi informacija. |
| **Saugumas** | reiškia informacijos saugumą suprantamą kaip procesų ir kontrolės priemonių derinį, įgyvendinamą siekiant apsaugoti informaciją nuo įvairių grėsmių ir užtikrinti jos konfidencialumą, vientisumą ir prieinamumą. |
| **Konfidencialumas** | reiškia patvirtintų apribojimų prieigoms bei informacijos atskleidimui išlaikymas ir taikymas, įskaitant priemones, skirtas asmens duomenų, teisės į privatumą bei Bendrovės konfidencialios informacijos apaugai. |
| **Politika** | reiškia šią Informacijos saugumo politiką |

# **TIKSLAS IR APIMTIS**

1. Šia Informacijos saugumo politika (toliau – **Politika**) yra siekiama nustatyti bendruosius saugumo reikalavimus Bendrovės pasitelkiamoms informacinėms technologijoms bei jų naudojimo būdams, siekiant užtikrinti maksimalų Bendrovės ir jos klientų, taip pat darbuotojų, kontrahentų bei kitų asmenų informacijos saugumą, ir apsaugoti juos nuo neteisėtų ir žalą sukeliančių tiesioginių ar netiesioginių, tyčinių ar atsitiktinių asmenų veiskmų tvarkant prieinamus asmens ir kitus duomenis, taip pat naudojant atitinkamą įrangą savo darbo funkcijoms atlikti.
2. Politikos tikslas yra apsaugoti Bendrovės klientus, darbuotojus, kontrahentus nuo neteisėtų ir žalą sukeliančių tiesioginių ir netiesioginių, tyčinių ar atsitiktinių asmenų veiksmų tvarkant jiems prieinamus asmens ar kitus duomenis, taip pat naudojant atitinkamą įrangą savo darbo funkcijoms atlikti.
3. Ši Politika yra taikoma tvarkant bet kuriose informacinėse sistemose esančią ir bet kurioje laikmenoje saugomą Bendrovės informaciją, nepriklausimai nuo to, ar šios informacijos tvarkymas yra susijęs su Bendrovės vidaus procesais, ar su Bendrovės išorės santykiais su bet kuriais trečiaisiais asmenimis.
4. Ši Politika pat pat yra taikoma Bandrovės darbuotojams jų darbo funkcijų vykdymo metu ir (ar) naudojant jiems Bendrovės suteiktą įrangą ir įrankius.
5. Ši Politika taikoma kartu su kitomis taisyklėmis, procedūromis ar kitais Bendrovės dokumentais.
6. Ši Politika yra taikoma ir Bendrovės vardu informaciją tvarkantiems paslaugų tiekėjams (įskaitant duomenų tvarkytojus)tiek, kiek Politikos nuostatos neprieštarauja sufarytai paslaugų teikimo, duomenų tvarkymo ar kitai sutarčiai.

# **INFORMACIJAI TVARKYTI NAUDJAMOS SISTEMOS**

1. Bet kokios informacinės sistemos, įskaitant, bet neapsiribojant, kompiuterine, serverių įranga, bet kokia programine įranga, operacinėmis sistemomis, bet kokiomis duomenų laikmenomis, tinko paskyromis, elektroninio pašto paskyromis, paieškos sistemomis ir bet kokia kita Bendrovės veikloje naudojama technine įranga ir įrankiais, yra laikomos Bendrovės nuosavybe:
   1. kiekvienas darbuotojas jam Bendrovės suteiktus įrenginius ir įrangą privalo naudoti atsakingai ir atidžiai, ir tik su Bendrovės veikla susijusiems tikslams. Vienintelė šios taisyklės išimtis yra atvejai, kai Bendrovė, suteikdama darbuotojui įrenginį (mobilų telefoną, nešiojamą ar planšetinį kompiuterį) leidžia jį naudoti ir asmeniniais tikslais.
   2. kiekvienas darbuotojui suteiktas įrenginys yra registruojamas.

DARBUOTOJŲ PAREIGOS

1. Visiems Bendrovės darbuotojams, kuriems teisės aktų ir (ar) sutartinių santykių pagrindu yra suteikta prieiga prie Bendrovės valdomos informacijos ar informacijos apdorojimo priemonių teisės aktuose ar sutartyje numatytoms funkcijoms atlikti, privalo laikytis šios Politikos nuostatų.
2. Bet kokia informacija, prieinama darbuotojui jo darbo funkcijų vykdymo metu, bus laikoma konfidencialia ir saugoma laikantis šios Politikos nuostatų. Informacija negali būti atskleidžiama jokiems tretiesiems asmenims, išskyrus atvejus, kai toks atskleidimas yra būtinas su Bendrovės veikla susijusiems tikslams ir ją gaunantys tretieji asmenys įsipareigoja užtikrinti tokios informacijos konfidencialumą. Darbuotojai dirbantys su tokia informacija privalo laikytis konfidencialumo principo. Šios pareigos lieka galioti ir pasibaigus darbo ar kitiems sutartiniams santykiams su Bendrove.
3. Visi fizinių asmenų prašymai, susiję su asmens duomenimis ir (ar) jų tvarkymu, kuriuos Bendrovės darbuotojas gauna vykdydamas savo darbo funkcijas, turi būti perduodami Bendrovės darbuotojui atsakingam už asmens duomenų tvarkymą.
4. Tais atvejais, kai jungdamiesi prie Bendrovės informacinių siistemų ar prieigai kitų išteklių (pvz. jungdamiesi prie darbinio elektroninio pašto), darbuotojai naudoja asmennius įrenginius ar įrangą, jie privalo laikytis šios Politikos nuostatų taip pat, kaip ir naudodamiesi Bendrovės suteiktais įrenginiais ar įranga. Draudžiama saugoti bet kokius su Bendrovės veikla susijusius duomenis ir (ar) informaciją darbuotojų asmeniniuose įrenginiuose ar įrangoje. Bet koks Bendrovės duomenų tvarkymas ir saugojimas yra galimas tik per Bendrovei priklausančius įrenginius.

PRIEIGŲ VALDYMAS IR INFORMACIJOS APSAUGA

1. Bet kokie įrenginiai bei informacija darbuotojams yra pasiekiami priklausomai nuo jų darbo funkcijų pobūdžio, turimų atsakomybių ir griežtai vadovaujamasi principu „būtina žinoti“. Prieiga prie konkrečios Bendrovės valdomos informacijos turi būti suteikta darbuotojui tik ta apimtimi, kuri reikalinga jo tiesioginėms funkcijoms atlikti.
2. Darbutojai, kurių kompiuteriuose saugomi klientų, kitų asmenų duomenys, arba iš kurių galima prisijunti prie Bnedorvės informacinių sistemų, savo kompiuterius turi apsaugoti slaptažodžiais. Neapsaugotos slaptažodžiais, vartotojų paskyros draudžiamos.
3. Darbuotojas yra atsakingas už visus veiksmus, atliekamus naudojantis jam paskirta paskyra. Kiekvienas darbuotojas privalo užtikrinti, kad jo paskyrų duomenys (slaptažodžiai) nebūtų prieinami jokiems tretiesiems asmenims, įskaitant kitus Bendrovės darbuotojus.
4. Prieigas prie informacinių sistemų apsaugantys slaptažodžiai turi būti sudaromi atsakingai (jie negali būti lengvai atspėjami) ir reguliariai keičiami ( ne rečiau kaip kartą per 6 mėnesius). Kiekvienas darbuotojas yra asmeniškai atsakingas už savonaudojamų slaptažodžių atitiktį šios Politikos nusotatoms ir kitoms Bendrovės taisyklėms.
5. Slaptažodis turi būti sudarytas iš mažiausiai 8 simbolių, iš kurių bent viens turi būti skaičius ir bent vienas turi būti raidė. Slaptažodį saugo ir jį gali žinoti tik darbuotojas, dirbantis su konkrečiu kompiuteriu ar sistema. Slaptažodis negali būti pasiekiamas kitiems asmenims (pvz., užrašomas ant lapelio ir paliekamas darbo vietoje).
6. Darbuotojas gali susipažinti su konfidencialia informacija tik tuo atveju, jeigu jis turi atitinkamus įgaliojimus pagal darbo sutartį ar tokius įgaliojimus jam suteikė Bendrovė.
7. Darbuotojai, atiekantys asmens duomenų tvarkymą, turi užkirsti kelią bet kokiam atsitiktiniam ar neteisėtam duomenų tvarkymui, tinkamai bei atsakingai saugoti dokumentus (vengti nereikalingų dokumentų kopijų su asmens duomenimis laikymoir kt.). Dokumentų, kuriuose yra asmens duomenų, kopijos turi būti sunaikinamos tokiu būdu, kad šių dokumentų ir jų turinio negalima būtų atkurti.
8. Nesant būtinybės, rinkmenos su klientų, kitų asmenų duomenimis neturi būti dauginamos skaitmeniniu būdu (neuturi būti daromos krinkmenų kopijos), saugomos kompiuterių kietuosiuose diskuose, nešiojamose laimenose.
9. Bendrovės darbuotojai privalo taip organizuoti savo darbą, kad kiek įmanoma būtų apribota galimybė kitiems asmenims (kitiems Bendrovės darbuotojams, paslaugų tiekėjams ir kitiems tretisiems asmenims) susipažinti su jų tvarkomais asmens duomenimis.
10. Tai įgvendinama nepaliekant dokumentų su asmens duomenimis ir įrenginių, kuriais naudojantis galima būtų susipažinti su asmens duomenimis be priežiūros, tokiu būdu, kad juose esančią informaciją galėtų perskaityti darbuotojai, neturintys teisės dirbti su konkrečiais asmens duomenimis ir kiti tretieji asmenys. Dokumenus laikyti taip, kad jų (ar jų fragmentų) negalėtų perskaityti atsitktiniai tretieji asmenys. Jeigu dokumentai, kuriuose yra asmens duomenys, jų gavėjams perduodami per asmenis neturinčiais teisės tvarkyti tokius asmens duomenis, arba paštu, ar per kurjerį, jie turi būti siunčiami užklijuotame, nepermatomame voke.
11. Darbuotojai gali perduoti dokumentus, kuriuose yra asmens duomenys, tik tiems darbuotojams, kurie pagal savo pareigas ar atskirus pavedimus turi teisę susipažinti su tais asmens duomenimis.
12. Darbuotjo prieigos teisės prie Bendrovės informacinės sistemos ar kitų išteklių turi būti nedelsiant panaikinamos, kai išnyksta pagrindas ar poreikis naudotis ta sistema ir (ar) tvarkyti joje esančius duomenis (pvz. pasibaigus darbo santykiams arba pasikeitus darbuotojo pareigoms ar darbo funkcijoms).

TECHNINĖS SAUGUMO PRIEMONĖS

1. Visiems bet kokiu būdu surinktiems ir tvarkomiems, bet kokios formos (popierinės, elektroninės ir kt.) duomenims ir informacijai yra taikomi šios Politikos ar atitinkamų teisės aktų reikalavimai dėl informacijos surinkimo, tvarkymo, apsaugos ir tolesnio saugojimo. Tokie duomenys ir informacija saugiai laikomi Bendrovės nustatytose vietose, laikantis taikytinuose teisės aktuose ir Bendrovės vidaus dokumentuose nustatytų terminų.
2. Bendrovės įrenginiai bei informacinės sistemos yra tinkamai apsaugoti techninėmis bei organizacinėmis priemonėmis siekiant išvengti neleistinos prieigos.
3. Perduodant asmens duomenis išoriniais perdavimo tinklais, yra užtikrinamas saugių slaptažodžių naudojimas.
4. Darbuotojų kompiuteriai, kuriuose yra saugomos rinkmenos su klientų, kitų fizinių ir (ar) juridinių asmenų duomenimis, negali būti laisvai pasiekiami ir prieinami iš kitų tinklo kompiuterių.
5. Jeigu Bendrovės duomenims pasiekti yra naudojami įvairūs nuotoliniai įrenginiai, darbuotojas privalo įsitikinti, kad naudojamas interneto ryšys yra saugus ir patikimas. Bendrovės duomenims pasiekti negali būti naudojamas viešas, neapsaugotas interneto ryšys.
6. Mobiliuosiuose įrenginiuose ( nešiojamuose kompiuteriuose, planšetėse, išmaniuosiuose telefonuose ir kt.) jei jie naudojami ne Bendrovės vidiniame kompiuterių tinkle, esantys asmens duomenys ir prisijungimo prie Bendrovės informacinių sistemų, duomenys turi būti saugomi kitomis priemonėmis, kurios atitiktų esamas rizikas.
7. Į Bendrovės įrenginius gali būti diegiamos ir juose naudojamos tik Bendrovės leidžiamos informacinės sistemos ir tinkamai licencijuota įranga. Bendrovės įrenginiai bei įranga yra tinkamai apsaugoti antivirusine ir (ar) kitokia programine įranga, skirta apsisaugoti nuo kenkėjiškos programinės įrangos.
8. Bendrovės naudojama programinė įranga yra atnaujinama pagal tiekėjų rekomendacijas.
9. Kai Bendrovės saugoma informacija tampa nebereikalinga vykdant Bendrovės veiklą, tokia informacija ištrinama, visos jos kopijos sunaikinamos, o su šios informacijos tvarkymu susiję darbuotojai atitinkamai informuojami apie jų pareigą ištrinti, sunaikinti ir (ar) grąžinti Bendrovei visą informaciją, kurios jiems nebereikia vykdant darbo funkcijas. Ypač kai nutrūksta darbo santykiai su darbuotoju.
10. Siekiant įvertinti šios Politikos reikalavimų laikymąsi bei įvertinti ar naudojamos saugumo priemonės yra pakankamos, atliekamas duomenų tvarkymo keliamos rizikos vertinimas.

DRAUDŽIAMI VEIKSMAI

1. Išskyrus konkrečiai nustatytas išimtis, jokiais atvejais ir jokiomis aplinkybėmis Bendrovei priklausantys įrenginiai, sistemos ir įrankiai negali būti naudojami su darbuotojų darbo funkcijomis ar Bendrovės veikla nesusijusiais tikslais.
2. Jokia šioje Politikoje nurodyta informacija negali būti siunčiama, perduodama arba bet kokiu kitu būdu atskleidžiama tretiesiems asmenims, nebent tai būtina darbuotojo darbo funkcijoms vykdyti ir tik tokia apimtimi, kokia reikalinga darbo funkcijų vykdymui. Duomenų perdavimo ar kitokio atskleidimo tretiesiems asmenims atveju turi būti užtikrinama, kad duomenys yra perduodami naudojant saugias priemones ir (ar) imamasi kitų reikiamų saugumo priemonių.
3. Darbuotojams draudžiama jų asmeniniuose įrenginiuose laikyti Bendrovės valdomus (tvarkomus) asmens duomenis ar bet kokią konfidencialią Bendrovės informaciją.
4. Griežtai draudžiami veiksmai, nenumatant jokių išimčių: bet kokio fizinio ar juridinio asmens intelektinės nuosavybės teisių pažeidimas, įskaitant, bet neapsiribojant, bet kokios nelegalios programinės įrangos, virtualių platformų ar kito Bendrovei nelicencijuoto skaitmeninio turinio įdiegimu, kopijavimu, platinimu ar saugojimu Bendrovės sistemose, įrangoje ar įrenginiuose.
5. Bet kurio asmens teisių pažeidimas dėl perteklinio ir nereikalingo jo asmens duomenų rinkimo ir tvarkymo.
6. Priėjimas prie Bendrovės duomenų, bet kokio įrenginio ar įrangos, prisijungimas ar pasinaudojimas paskyra kitais nei Bendrovės veiklos užtikrinimo ar konkretaus darbuotojo darbo funkcijų vykdymo užtikrinimo tikslais.
7. Darbuotojo paskyros slaptažodžio atskleidimas kitiems asmenims ir (ar) leidimas kitiems asmenims naudotis tokia darbuotojo paskyra.
8. Visais atvejais griežtai draudžiama naudotis viešais prieigos įrenginiais (pvz. bibliotekose, kitose viešose erdvėse). Jeigu suteiktomis darbo priemonėmis, darbo funkcijų vykdymui, naudojamasi viešose vietose, darbuotojai privalo dėti pastangas, kad jų įrenginio ekrane esama (tvarkoma) informacija nebūtų matoma, stebima ar įrašinėjama pašalinių asmenų, taip pat nebūtų jungiamasi, naudojant viešu, nesaugiu belaidžiu interneto ryšiu.

BAIGIAMOSIOS NUOSTATOS

1. Bet koks informacijos saugumo normų pažeidimas laikomas informacijos incidentu, kuris gali daryti neigiamą įtaką Bendrovės veiklos tęstinumui.
2. Apie visus informacijos saugumo incidentus turi būti nedelsiant pranešta atsakingam Bendrovės darbuotojui ir Bendrovės vadovui, kurie atitinkamai imasi priemonių galimai žalai išvengti, kilusiai žalai pašalinti ir buvusiai saugumo būklei atkurti.
3. Kai yra būtina, Bendrovės vadovas privalo užtikrinti, kad apie informacijos saugumo pažeidimus būtų pranešta kompetentingoms institucijoms.
4. Už visų šioje Politikoje nurodytų saugumo priemonių įgyvendinimą yra atsakinga Bendrovė ir (ar), kai taikytina, jos pasitelkti paslaugų teikėjai.
5. Politika tvirtinama ir keičiama Bandrovės vadovo sprendimu.
6. Ši Politika yra peržiūrima pasikeitus asmens duomenų ar dokumentų saugojimo aplinkybėms ar teisės aktų reikalavimams, ir prireikus atitinkamai atnaujinama.
7. Politika peržiūrima ne rečiau kaip kas 3 metus ir atnaujinama pagal poreikį.
8. Su Politika yra supažindinami priimami ir esami Bendrovės darbuotojai.