PATVIRTINTA
SĮ „Susisiekimo paslaugos“ valdybos
2021 m. gegužės 13 d. sprendimu Nr. 2021-V-8-7

Savivaldybės įmonės „Susisiekimo paslaugos“

Informacijos saugumo politika

TURINYS

1. ĮVADAS

1.1. Informacija yra vertinga Savivaldybės įmonės „Susisiekimo paslaugos“ turto dalis, todėl jos praradimas, neteisėtas pakeitimas ar atskleidimas, sugadinimas ar informacijos apdorojimo nutraukimas gali sukelti Savivaldybės įmonės „Susisiekimo paslaugos“ veiklos sutrikimų, padaryti žalos kitiems fiziniams ir juridiniams asmenims. Atsižvelgdama į tai, Savivaldybės įmonė „Susisiekimo paslaugos“ imasi priemonių informacijos saugumui užtikrinti.

1.2. Informacijos saugumo valdymo tikslas – užtikrinti tinkamą ir efektyvų informacijos saugumo valdymą ir išvengti veiklos sutrikdymo bei žalos atsiradimo dėl informacijos konfidencialumo, vientisumo bei prieinamumo pažeidimų.

2. SĄVOKOS

2.1. Informacijos saugumo politikoje naudojamos sąvokos:

2.1.1. Įmonė – Savivaldybės įmonės „Susisiekimo paslaugos“.

2.1.2. Informacija – tikslingi, prasmę turintys duomenys, kurie gali egzistuoti įvairiomis formomis, pvz., atspausdinti, rašyti ranka, žodiniai, sugeneruoti elektroniniu būdu ar saugomi. Informacija šios Politikos kontekste yra laikomi tiek asmens duomenys, tiek bet kokia kita su Įmonės veikla susijusi informacija.

2.1.3. Informacijos saugumas – procesų ir kontrolės priemonių derinys, įgyvendinamas siekiant apsaugoti informaciją nuo įvairių grėsmių ir užtikrinti jos konfidencialumą, vientisumą ir prieinamumą.

2.1.4. Asmens duomenys – bet kokia informacija apie fizinį asmenį, kurio tapatybė nustatyta arba kurio tapatybę galima nustatyti (duomenų subjektas); fizinis asmuo, kurio tapatybę galima nustatyti, yra asmuo, kurio tapatybę tiesiogiai arba netiesiogiai galima nustatyti, visų pirma pagal identifikatorių, kaip antai vardą ir pavardę, asmens identifikavimo numerį, buvimo vietos duomenis ir interneto identifikatorių arba pagal vieną ar kelis to fizinio asmens fizinės, fiziologinės, genetinės, psichinės, ekonominės, kultūrinės ar socialinės tapatybės požymius.

2.1.5. Konfidencialumas – patvirtintų apribojimų prieigoms bei informacijos atskleidimui išlaikymas ir taikymas, įskaitant priemones, skirtas asmens duomenų, teisės į privatumą bei Įmonės konfidencialios informacijos apsaugai.

2.1.6. Trečioji šalis – juridinis ar fizinis asmuo, kuriam suteikiama prieiga prie Įmonės informacijos ar turto, įskaitant, bet neapsiribojant, išoriniais paslaugos teikėjais, konsultantais, klientais, partneriais, laisvai samdomais asmenimis.

2.1.7. Turtas – materialios ar nematerialios vertės objektas, įskaitant, bet neapsiribojant žmonėmis, informacija, technine ar programine įranga, įrenginiais, procedūromis, pastatais, infrastruktūra, užsakomosiomis paslaugomis, intelektine nuosavybe, tinklais.

2.1.8. Politika – ši informacijos saugumo politika.

3. INFORMACIJOS SAUGUMO VALDYMO SISTEMA

3.1 Įmonės tvarkomos informacijos saugumas apima tris pagrindinius aspektus:

3.1.1 konfidencialumą – informacijos apsaugą nuo nesankcionuoto atskleidimo;

3.1.2 vientisumą – informacijos apsaugą nuo nesankcionuoto ar atsitiktinio pakeitimo;

3.1.3 prieinamumą – užtikrinimą, kad informacija prieinama tada, kai ji yra reikalinga.

3.2 Įmonės Informacijos saugumo valdymo sistema (toliau – ISVS) įgyvendina šią Politiką ir apibrėžia pagrindinius Informacijos saugumo užtikrinimo bei valdymo principus.

3.3 Įmonės ISVS reikalavimai nustatomi vadovaujantis:

3.3.1 Europos Sąjungos ir Lietuvos Respublikos teisės aktais, reglamentuojančiais Informacijos saugumą ir asmens duomenų tvarkymą, įskaitant Bendrąjį duomenų apsaugos reglamentą (ES) 2016/679 (toliau – BDAR);

3.3.2 Valstybinės duomenų apsaugos inspekcijos ir Europos duomenų apsaugos valdybos metodiniais nurodymais bei kitais teisės šaltiniais, susijusiais su Informacijos tvarkymu ir saugumu;

3.3.3 Įmonės strateginiais tikslais;

3.3.4 Įmonės skaitmenine strategija.

3.4 Įmonės reikalavimai taikomi:

3.4.1 visiems Įmonės veiklos procesams ir visiems struktūriniams padaliniams;

3.4.2 visai Įmonės Informacijai, nepriklausomai nuo jos formos ir saugojimo būdo;

3.4.3 visiems Įmonės darbuotojams ir Tretiesiems asmenims, kuriems teisės aktų ir (ar) sutartinių santykių pagrindu yra suteikta prieiga prie Įmonės Informacijos ar Informacijos apdorojimo priemonių teisės aktuose ar sutartyje numatytoms funkcijoms (teisėms) atlikti;

3.4.4 išorinių paslaugų teikėjų teikiamoms paslaugoms.

3.5 Įmonės ISVS siekia tokių Informacijos saugumo tikslų:

3.5.1 užtikrinti ir valdyti Informacijos saugumą, atsižvelgiant į Įmonės strateginius tikslus, galiojančius ir Įmonės taikomus Europos Sąjungos ir Lietuvos Respublikos teisės aktus, ypač BDAR;

3.5.2 užtikrinti ir valdyti atitikimą išoriniams ir vidiniams Informacijos saugumo reikalavimams, atliekant periodinį atitikties vertinimą ir šalinant nustatytus trūkumus;

3.5.3 užtikrinti Informacijos saugumo pažeidimų sprendimą ir jų priežasčių pašalinimą, įgyvendinant incidentų valdymo procesą;

3.5.4 užtikrinti tinkamą Informacijos saugumo ir apdorojimo priemonių parinkimą ir įgyvendinimą;

3.5.5 užtikrinti taikomų Informacijos saugumo priemonių veiksmingumą.

3.6 Įmonė įsipareigoja užtikrinti tinkamą ir efektyvų Informacijos saugumo valdymą, siekdama išvengti veiklos sutrikdymo dėl konfidencialios Informacijos atskleidimo, Informacijos vientisumo pažeidimo arba Informacijos neprieinamumo dėl jos praradimo ar sistemų neveikimo.

3.7 Informacijos saugumas valdomas nuosekliai planuojant, įgyvendinant, tikrinant ir nuolatos gerinant ISVS.

3.8 Bet koks Informacijos saugumo normų pažeidimas laikomas Informacijos saugumo incidentu, kuris gali daryti neigiamą įtaką Įmonės veiklos tęstinumą bei sugadinti / pakenkti organizacijos įvaizdžiui visuomenėje.

3.9 Įmonės darbuotojams ir Trečiosioms šalims, pažeidusiems ISVS reikalavimus, yra taikomos Lietuvos Respublikos įstatymuose numatytos priemonės.

3.10 ISVS sudaro šios Politikos 4 skyriuje nurodyti dokumentai.

4. INFORMACIJOS SAUGUMO VALDYMO SISTEMOS DOKUMENTAI

5.1. Politikos nuostatos yra įgyvendinamos patvirtinant Įmonės vidaus teisės aktus, pagrindiniai tvirtinami Įmonės vidaus teisės aktai nurodyti Priede Nr. 1.

5. BAIGIAMOSIOS NUOSTATOS

5.2. Politika tvirtinama ir keičiama Įmonės valdybos sprendimu.

5.3. Už Politikos įgyvendinimo kontrolę atsako Technologijų skyriaus vadovas.

5.4. Politika peržiūrima ne rečiau kaip kas 3 metus ir atnaujinama pagal poreikį.

5.5. Su Politika yra supažindinami priimami ir esami Įmonės darbuotojai.

5.6. Politika yra skelbiama viešai Įmonės interneto svetainėje.

Priedas Nr. 1

Informacijos saugumo valdymo sistemos dokumentai

Eil. Nr.	Dokumento pavadinimas	Dokumento aprašymas
1.	Asmens duomenų tvarkymo taisyklės	Reglamentuoja visus asmens duomenų tvarkymo Įmonės tikslus, Įmonės valdomų asmens duomenų kategorijas, duomenų subjektų teises ir kitus su asmens duomenų apsauga susijusius įmonės įsipareigojimus
2.	Informacijos saugumo organizavimo aprašas	
3.	Informacijos saugumo diegiant informacines sistemas taisyklės	
4.	Mobilaus ir internetinio ryšio saugumo reikalavimai	Reikalavimai mobilaus ir interneto ryšio saugumo užtikrinimui
5.	Informacinių sistemų saugumo testavimo reikalavimai	
6.	Prieigos prie duomenų kontrolės taisyklės ir prieigų matrica	Nustato prieigų prie Įmonės valdomų asmens duomenų išdavimo / keitimo / naikinimo taisykles ir detalizuoja bendrąsias prieigų teises pagal Įmonėje patvirtintas pareigybes
7.	Darbuotojo darbo priemonių ir prieigų sąrašas	
8.	Prisijungimo prie informacinių sistemų ir darbo vietų slaptažodžių taisyklės	Visiems prie Įmonės informacinių sistemų ir darbo vietų prisijungiantiems asmenims taikomos slaptažodžių kūrimo ir keitimo taisyklės
9.	Techninių ir organizacinių priemonių, taikomų SĮ „Susisiekimo paslaugos“ tiekėjams, aprašas	Būtinųjų techninių ir organizacinių priemonių, kurias savo veikloje privalo taikyti Įmonės tiekėjai, kad Įmonė galėtų naudotis tik duomenų apsaugos reikalavimus atitinkančių įmonių paslaugomis, aprašymas
10.	Informacinių sistemų (IS) naudotojų administravimo taisyklės	Visiems Įmonės IS naudotojams, administratoriams ir informacijos tvarkytojams, dirbantiems su Įmonės IS, taikomos taisyklės
11.	Savivaldybės įmonės „Susisiekimo paslaugos“ reagavimo į asmens duomenų saugumo pažeidimus procedūros aprašas	Nustato darbuotojų veiksmus, įvykus duomenų saugumo pažeidimui, jų išaiškinimo, pranešimo priežiūros institucijai, duomenų subjektams tvarką, pažeidimo prevencinio plano sudarymą bei kitus atvejus
12.	Informacijos saugumo incidentų valdymo planas ir informacinių sistemų veiklos atkūrimo detalusis planas	Nustato saugumo incidento atvejų fiksavimą, reagavimą bei darbuotojų veiksmus, įvykus incidentui
13.	Prieigos prie informaciją apdorojančių įrenginių taisyklės	
14.	Savivaldybės įmonės „Susisiekimo paslaugos“ informacinių ir komunikacinių technologijų naudojimo bei darbuotojų stebėsenos ir kontrolės darbo vietoje tvarka	Siekiant apsaugoti Įmonės konfidencialią informaciją ir valdomus asmens duomenis, visiems Įmonės darbuotojams taikomos technologijų naudojimo taisyklės ir aprašomi atvejai, kada Įmonė turi teisę tikrinti darbuotojų kompiuterizuotą darbo vietą bei kitus duomenis.