PATVIRTINTA
Akcinės bendrovės Lietuvos pašto valdybos
2024 m. lapkričio 20 d. nutarimu Nr. 15-44

INFORMACIJOS SAUGUMO POLITIKA

Versija 4

Įsigalioja nuo 2024-11-20

INFORMATION SECURITY POLICY

Politikos savininkas: Saugos ir prevencijos departamentas

Tikslas:	Nustatyti principus ir priemones, kurie užtikrintų informacijos konfidencialumą, vientisumą ir prieinamumą, nes tai esminės prielaidos ilgalaikėms Bendrovės verslo operacijoms, reputacijos palaikymui bei teisiniam ir finansiniam saugumu.
Taikymo apimtis:	Informacijos saugumo politika taikoma visoje Bendrovės veikloje bei visiems Bendrovės darbuotojams.

TURINYS

DOKUMENTO ISTORIJA

Pasirašymo data	Versija	Esminis dokumento keitimo aprašymas	Dokumento savininkas	Dokumento rengėjas
2024-11-20	V4	Peržiūrėta, papildyta reikalavimu peržiūrėti ne rečiau kaip kartą per metus bei pagal naujausias Valstybinės duomenų apsaugos inspekcijos rekomendacijas.	Saugos ir prevencijos departamentas	Ekspertas
2021-10-20	V3	Peržiūrėta, papildyta teisinio reguliavimo sritis.	Saugos ir prevencijos departamentas	Ekspertas
2020-12-17	V2	Sukurta visiškai nauja politikos versija, senoji politika transformuojama į „Bendrųjų informacijos saugos reikalavimų tvarką“.	Saugos ir prevencijos departamentas	Ekspertas
2018-02-14	V1	Pirminė politikos versija.	Saugos ir prevencijos departamentas	Ekspertas

I. BENDROSIOS NUOSTATOS

1.1. Bendrovės taikomoje informacijos saugumo valdymo sistemoje bei šioje Politikoje numatyti pagrindiniai principai ir priemonės, kuriais remiantis užtikrinamas informacijos saugumas, įskaitant ir kibernetinio saugumo sritį bei asmens duomenų saugumo užtikrinimą. Ši Politika parengta remiantis žemiau nurodytais teisės aktais bei juos įgyvendinančiais teisės aktais, priežiūros institucijų dokumentais ir bei tarptautinių įmonių gerosiomis praktikomis.

II. REGULIAVIMO SRITIS

2.1.1. LR kibernetinio saugumo įstatymas;
2.1.2. 2020 m. lapkričio 26 d. Lietuvos banko valdybos nutarimas Nr. 03-174 „Dėl Informacinių ir ryšių technologijų ir saugumo rizikos valdymo reikalavimų aprašo patvirtinimo;
2.1.3. 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB;
2.1.4. LR asmens duomenų teisinės apsaugos įstatymas.

III. SĄVOKOS IR SANTRUMPOS

3.1. Šioje akcinės bendrovės Lietuvos pašto informacijos saugumo politikoje (toliau – Politika) vartotinos sąvokos turi būti suprantamos ir aiškinamos kaip nurodyta toliau:

„Bendrovė“	Akcinė bendrovė Lietuvos paštas (kodas 121215587, registruotos buveinės adresas Juozo Balčikonio g. 3, Vilnius), įskaitant ir visas dukterines įmones
„Darbuotojas, atsakingas už informacijos saugumo funkcijos vykdymą“	Darbuotojas, kuriam pareiginiuose nuostatuose arba Bendrovės generalinio direktoriaus įsakymu paskirtas informacijos saugumo funkcijų vykdymas.
„Asmens duomenys“	Bet kuri informacija, susijusi su fiziniu asmeniu – duomenų subjektu, kurio tapatybė yra žinoma arba gali būti tiesiogiai ar netiesiogiai nustatyta pasinaudojant tokiais duomenimis kaip asmens kodas, vienas arba keli asmeniui būdingi fizinio, fiziologinio, psichologinio, ekonominio, kultūrinio ar socialinio pobūdžio požymiai;
„Informacijos saugumas“	Organizacinių bei techninių priemonių visuma, apimanti informacijos, įskaitant asmens duomenų, valdymo procese dalyvaujančius procesus, technologijas ir asmenis bei skirta išsaugoti informacijos, įskaitant asmens duomenų, konfidencialumą, vientisumą ir prieinamumą;
„Informacijos saugumo valdymo sistema“	Organizacinių ir techninių priemonių visuma, kurios tikslas yra efektyviai užtikrinti informacijos, įskaitant asmens duomenis, saugumą Bendrovėje;
„Prieiga“	Galimybė tvarkyti duomenis informacinėse sistemose;
„Konfidencialumas“	Užtikrinimas, kad informacija, įskaitant asmens duomenis, būtų prieinama tik įgaliotiems asmenims, turintiems prieigos prie informacijos teisę;
„Prieinamumas“	Užtikrinimas, kad įgaliotieji naudotojai, kai reikia turi prieigą prie reikalingų informacinių resursų;
„Vientisumas“	Informacijos, įskaitant asmens duomenų, ir apdorojimo metodų tikslumo ir išbaigtumo užtikrinimas;
„Funkcijų atskyrimo“ principas	Siekis užkirsti kelią nepagrįstai prieigai prie didelio duomenų kiekio arba prieigos teisių derinių paskirstymui, kuriuo gali būti naudojamasi siekiant išvengti kontrolės priemonių;

„Mažiausios privilegijos“ principas	Informacinių ir ryšių technologijų vartotojams turi būti suteikiamos minimalios prieigos teisės, reikalingos jų būtinoms pareigoms vykdyti;
„Pritaikytoji duomenų apsauga“	Planuojant naują būdu tvarkyti asmens duomenis, į duomenų apsaugą yra atsižvelgiama pradiniuose tokio planavimo etapuose;
„Standartizuotoji duomenų apsauga“	Nustatant standartizuotąsias asmens duomenų tvarkymo priemones, parenkamos tokios priemonės, kurios padeda užtikrinti kuo didesnę privatumo apsaugą.

IV. POLITIKOS TIKSLAI, ĮGYVENDINIMAS IR KONTROLĖ

4.1. Politikos tikslai

4.1.1. Nustatyti priemones, kurios užtikrintų informacijos, įskaitant asmens duomenų, konfidencialumą, vientisumą ir prieinamumą, nes tai esminės prielaidos ilgalaikėms Bendrovės verslo operacijoms, reputacijos palaikymui bei teisiniam ir finansiniam saugumui;

4.1.2. Užtikrinti tokią informacijos saugumo valdymo sistemą, kuri būtų pagrista rizikų valdymu bei proaktyviai ir subalansuotai apimtų visas informacijos saugumui įtaką turinčias sritis – procesus, technologijas bei žmones (darbuotojus, klientus, trečiųjų šalių atstovus);

4.1.3. Užtikrinti, kad Bendrovės vidaus dokumentuose būtų nustatyti išsamūs informacijos saugumo reikalavimai, funkcijos, atsakomybės, atskaitomybės bei kontrolės priemonės;

4.1.4. Užtikrinti, kad Bendrovėje būtų kuriama informacijos saugumo kultūra, paremta pagarba Bendrovės klientų bei darbuotojų informacijos ir asmens duomenų konfidencialumui, veiklos bei operacijų tęstinumui;

4.2. Politikos taikymas

4.2.1. Politika ir ją įgyvendinantys Bendrovės vidaus dokumentai yra aktualūs ir taikomi visiems Bendrovės darbuotojams, procesams ir pokyčiams.

4.3. Politikos viešinimas

4.3.1. Politika yra skelbiama Bendrovės intranete ir Bendrovės oficialiame tinklalapyje www.lietuvospastas.lt .

4.4. Politikos įgyvendinimo priežiūra ir kontrolė

4.4.1. Politikos nuostatų įgyvendinimas detalizuojamas kitose Bendrovės dokumentuose, kuriuos rengia už atitinkamas sritis atsakingi darbuotojai ir tvirtina Lietuvos pašto generalinis direktorius.

4.4.2. Už Politikos rengimą ir savalaikį atnaujinimą atsakingas Saugos ir prevencijos departamentas.

4.4.3. Politiką tvirtina Bendrovės valdyba.

4.4.4. Politika privalo būti peržiūrima ne rečiau nei kartą per metus ir atnaujinama poreikiui esant.

V. **INFORMACIJOS SAUGUMO UŽTIKRINIMO PRINCIPAI**

5.1. Informacijos saugumo rizikų vertinimas bei jų valdymas. Tai esminis pagrindas, užtikrinant optimalų balansą tarp verslo poreikių bei proporcingų informacijos saugumo reikalavimų nustatymo ir priemonių diegimo.
5.2. Prioritetų nustatymas prevencinių priemonių naudojimui, tokiu būdu efektyviausiai eliminuojant ar maksimaliai sumažinant informacijos saugos rizikas.
5.3. Informacijos bei informacinių sistemų klasifikavimas pagal jos svarbą konfidencialumo, vientisumo bei prieinamumo pažeidimams.
5.4. Prieigų taikymas visai klasifikuotai informacijai, įskaitant asmens duomenims, išlaikant „mažiausios privilegijos“ bei „funkcijų atskyrimo“ principus.
5.5. Daugiapakopių viena kitą papildančių saugumo priemonių taikymas saugant Bendrovės tinklą nuo kibernetinių atakų.
5.6. Visų lygių vadovų įsitraukimas – pavyzdžio demonstravimas bei užtikrinimas, kad taisyklių bei reikalavimų yra laikomasi.
5.7. Bendrajame duomenų apsaugos reglamente numatytų „pritaikytos duomenų apsaugos“ bei „standartizuotos duomenų apsaugos“ principų taikymas Bendrovės veikloje bei bet kuriame jos pokytyje.
5.8. Bendrovės turto ir išteklių, naudojamų informacijai ir asmens duomenims tvarkyti, registravimas, valdymas, reguliari peržiūra ir atnaujinimas.
5.9. Atsarginių kopijų darymas, šio proceso stebėsena, reguliarus testavimas, tinkamas kopijų laikymas.
5.10. Informacijos, įskaitant asmens duomenų, perdavimas teisės aktų nustatytais atvejais ir tvarka. Duomenų tvarkymui pasitelkiami tik tie tretieji asmenys, kurie užtikrina tinkamų techninių ir organizacinių priemonių įgyvendinimą ir atliekamo duomenų tvarkymo atitiktį teisės aktų reikalavimams. Bendrovės tvarkomų asmens duomenų gavėjai ir duomenų tvarkytojai detalizuojami Bendrovės vidaus dokumentuose.
5.11. Dokumentuotas pažeidimų valdymo ir pranešimo apie juos priežiūros institucijoms bei duomenų subjektams procesas. Pažeidimų, su pažeidimu susijusių faktų, jų poveikio (pavojaus fizinio asmens laisvėms ir teisėms lygio) ir taisomųjų veiksmų bei priemonių, kurių buvo imtasi registravimas ir dokumentavimas.
5.12. Bendrovės bei kiekvieno darbuotojo informacijos saugumo kultūros formavimas, pareigų (funkcijų) ir atsakomybių nustatymas.

VI. **INFORMACIJOS SAUGUMO SISTEMOS VALDYMAS**

6.1. Informacijos saugumo sistemos valdymo funkcijos yra deleguojamos visiems Bendrovės padaliniams priklausomai nuo jų atliekamų funkcijų. Bendrovės generalinio direktoriaus sprendimu yra paskiriami konkretūs Bendrovės padaliniai (pvz., departamentai, skyriai, grupės), kurie yra atsakingi už šias funkcijas:
   6.1.1. Informacijos saugumo rizikų vertinimas bei reikalavimų nustatymas;
   6.1.2. Informacijos klasifikavimas bei prieigų nustatymas;
   6.1.3. Techninių priemonių parinkimas ir diegimas;
   6.1.4. Darbuotojų kvalifikacija, mokymai, patikimumas;
   6.1.5. Reikalavimų pakankamumo, jų įgyvendinimo ir vykdymo kontrolė;
6.2. Bendrovės informacijos saugos sistemos valdymas vykdomas taikant Bendrovės veikloje organizacinių bei techninių priemonių visumą:
   6.2.1. Šią Politiką bei kitus vidaus dokumentus, reglamentuojančius informacijos saugos valdymą;
   6.2.2. Diegiant technines saugumo priemones, kurios užtikrina numatytų organizacinių priemonių vykdymą;
   6.2.3. Atliekant naudojamų priemonių pakankamumo bei veiksmingumo kontrolę;
   6.2.4. Atliekant reikalingus pakeitimus reikalavimų, procesų bei technologijų srityse.

VII. ATSKAITOMYBĖ BEI KONTROLĖ

7.1. Bendrovėje į informacijos saugumo funkcijos vykdymą skirtingu lygiu ir apimtimi įtraukiami:

7.1.1. **Valdyba** – tvirtina Informacijos saugumo politiką, kurioje nustatyti tikslai ir principai. Valdyba taip pat vykdo informacijos saugumo funkcijos stebėseną;

7.1.2. **Generalinis direktorius** - užtikrina valdybos nustatytų informacijos saugumo funkcijos tikslų ir principų įgyvendinimą Bendrovės veikloje, tvirtina Informacijos saugumo politiką įgyvendinančius vidaus dokumentus;

7.1.3. **Darbuotojas, atsakingas už informacijos saugumo funkcijos vykdymą** – atsakingas už šios funkcijos veikimą, šios funkcijos tobulinimą Bendrovėje.

7.2. Darbuotojas, atsakingas už informacijos saugumo funkcijos vykdymą, vieną kartą į metus teikia informacijos saugumo ataskaitą Bendrovės valdybai. Šis darbuotojas, kai objektyviai būtina, turi teisę kreiptis į valdybą ir pateikti informaciją dažnesniu periodiškumu.

7.3. Vadovaudamasi Bendrovei taikomu Nacionalinio kibernetinio saugumo centro (NKSC) bei Lietuvos banko (LB) reguliavimu, Bendrovė užtikrina periodinį audito atlikimą informacijos saugumo srityje.

VIII. BAIGIAMOSIOS NUOSTATOS

8.1. Atsižvelgiant į plačią informacijos saugumo priemonių apimtį ir kitus objektyvius kriterijus, šios Politikos nuostatos detalizuojamos ir įgyvendinamos priimant Bendrovės vidaus dokumentus (pvz., tvarkas, procesus, instrukcijas ir pan.).