PATVIRTINTA
Akcinės bendrovės Lietuvos pašto valdybos
2020 m. gruodžio 17 d. nutarimu Nr. 11-53

AKCINĖS BENDROVĖS LIETUVOS PAŠTO INFORMACIJOS SAUGUMO POLITIKA

1. SĄVOKOS

1.1. 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 J. Jasinskio g. 16, Vilnius;
„Darbuotojas, atsakingas už informacijos saugumo funkcijos vykdymą“	Bendrovės generalinio direktoriaus įsakymu paskirtas darbuotojas, atsakingas už informacijos saugumo funkcijos vykdymą.
„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 valdymo procese dalyvaujančius procesus, technologijas ir asmenis bei skirta išsaugoti informacijos konfidencialumą, vientisumą ir prieinamumą;
„Informacijos saugumo valdymo sistema“	Organizacinių ir techninių priemonių visuma, kurios tikslas yra efektyviai užtikrinti informacijos saugumą organizacijoje;
„Prieiga“	Galimybė tvarkyti duomenis informacinėse sistemose;
„Konfidencialumas“	Užtikrinimas, kad informacija 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 ir apdorojimo metodų tikslumo ir išbaigtumo užtikrinimas;
„Funkcijų atskyrimo“ principas	Siekis užkirsti kelią nepagrįstai prieigai prie didelio duomenų kieko 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 nauju 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.

2. BENDROSIOS NUOSTATOS

2.1. 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 praktinį (ne teisinį) 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.

2.2. **Reguliavimo sritis:**

2.2.1. 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;
2.2.2. LR asmens duomenų teisinės apsaugos įstatymas;
2.2.3. LR kibernetinio saugumo įstatymas;

2.2.4. 2020 m. lapkričio 26 d. Lietuvos banko valdybos nutarimas Nr. 03-174 „Dėl Informacinių ir ryšių technologijų ir saugumo rizikos valdymo reikalavimų aprašo patvirtinimo“;
2.2.5. Standartas LST ISO/IEC 27001-2014 „Informacinės technologijos. Saugumo metodai. Informacijos saugumo valdymo sistemos, kurio reikalavimai" (tapatus ISO/IEC 27001:2013).

2.3. Politikos tikslai

2.3.1. Nustatyti priemones, kurios užtikrintų informacijos konfidencialumą, vientisumą ir prieinamumą, nes tai esminės prielaidos ilgalaikėms Bendrovės verslo operacijoms, reputacijos palaikymui bei teisiniam ir finansiniam saugumui;
2.3.2. 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);
2.3.3. Užtikrinti, kad Bendrovės vidaus dokumentuose būtų nustatyti išsamūs informacijos saugumo reikalavimai, funkcijos, atsakomybės, atskaitomybės bei kontrolės priemonės;
2.3.4. Užtikrinti, kad Bendrovėje būtų kuriama informacijos saugumo kultūra, paremta pagarba Bendrovės klientų bei darbuotojų informacijos konfidencialumui, veiklos bei operacijų tęstinumui;

2.4. Politikos taikymas

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

2.5. Politikos viešinimas

Politika yra skelbiama Bendrovės dokumentų valdymo sistemoje ir prieinama visiems darbuotojams bei Bendrovės interneto puslapyje www.lietuvospastas.lt.

2.6. Politikos sudarymas ir keitimas

Politiką rengia, reguliariai peržiūri ir, jei reikalinga, atnaujina Bendrovės Darbuotojas, atsakingas už informacijos saugumo funkcijos vykdymą. Šią politiką tvirtina Bendrovės valdyba.

3. INFORMACIJOS SAUGUMO UŽTIKRINIMO PRINCIPAI

3.1. 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.
3.2. Prioritetų nustatymas prevencinių priemonių naudojimui, tokiu būdu efektyviausiai eliminuojant ar maksimaliai sumažinant informacijos saugos rizikas.
3.3. Informacijos bei informacinių sistemų klasifikavimas pagal jos svarbą konfidencialumo, vientisumo bei prieinamumo pažeidimams.
3.4. Prieigų taikymas visai klasifikuotai informacijai išlaikant „mažiausios privilegijos“ bei „funkcijų atskyrimo“ principus.
3.5. Daugiapakopių viena kitą papildančių saugumo priemonių taikymas saugant Bendrovės tinklą nuo kibernetinių atakų.
3.6. Visų lygių vadovų įsitraukimas – pavyzdžio demonstravimas bei užtikrinimas, kad taisyklių bei reikalavimų yra laikomasi.
3.7. Bendrajame duomenų apsaugos reglamente numatytų „pritaikytos duomenų apsaugos“ bei „standartizuotos duomenų apsaugos“ principų taikymas Bendrovės veikloje bei bet kuriame jos pokytyje.
3.8. Organizacijos bei kiekvieno darbuotojo informacijos saugumo kultūros formavimas.

4. INFORMACIJOS SAUGUMO SISTEMOS VALDYMAS

4.1. 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:
4.1.1. Informacijos saugumo rizikų vertinimas bei reikalavimų nustatymas;
4.1.2. Informacijos klasifikavimas bei prieigų nustatymas;
4.1.3. Techninių priemonių parinkimas ir diegimas;

4.1.4. Darbuotojų kvalifikacija, mokymai, patikimumas;
4.1.5. Reikalavimų pakankamumo, jų įgyvendinimo ir vykdymo kontrolė;
4.2. Bendrovės informacijos saugos sistemos valdymas vykdomas taikant Bendrovės veikloje organizacinių bei techninių priemonių visumą:
4.2.1. Šią Politiką bei kitus vidaus dokumentus, reglamentuojančius informacijos saugos valdymą;
4.2.2. Diegiant technines saugumo priemones, kurios užtikrina numatytų organizacinių priemonių vykdymą;
4.2.3. Atliekant naudojamų priemonių pakankamumo bei veiksmingumo kontrolę;
4.2.4. Atliekant reikalingus pakeitimus reikalavimų, procesų bei technologijų srityse.

5. ATSAKOMYBĖ, ATSKAITOMYBĖ IR KONTROLĖ

5.1. Bendrovėje į informacijos saugumo funkcijos vykdymą skirtingu lygiu ir apimtimi įtraukiami:
5.1.1. **Valdyba** – tvirtina Informacijos saugumo politiką, kurioje nustatyti tikslai ir principai. Valdyba taip pat vykdo informacijos saugumo funkcijos stebėseną;
5.1.1. **Audito ir rizikos valdymo komitetas** – stebi ir vertina informacijos saugumo funkcijos vykdymą Bendrovėje, teikia nuomonę, komentarus, pasiūlymus;
5.1.2. **Generalinis direktorius** - užtikrina valdybos nustatytų informacijos saugumo funkcijos tikslų ir principų įgyvendinimą Bendrovės veikloje, tvirtina Informacijos saugumo politiką įgyvendinančius vidaus dokumentus;
5.1.3. **Darbuotojas, atsakingas už informacijos saugumo funkcijos vykdymą** – atsakingas už šios funkcijos veikimą, šios funkcijos tobulinimą Bendrovėje.
5.2. Darbuotojas, atsakingas už informacijos saugumo funkcijos vykdymą, vieną kartą į metus teikia informacijos saugumo ataskaitą Bendrovės valdybai ir Audito ir rizikos valdymo komitetui. Šis darbuotojas, kai objektyviai būtina turi teisę kreiptis į valdybą ir pateikti informaciją kitu nei šiame punkte nurodytu periodiškumu.
5.3. Vadovaudamasi Bendrovei taikomu Lietuvos banko reguliavimu, Bendrovė užtikrina periodinį audito atlikimą informacijos saugumo srityje.

6. BAIGIAMOSIOS NUOSTATOS

6.1. 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.).

_____

Dokumentą elektroniniu parašu pasirašė MINDAUGAS,KYGUOLIS
Data: 2020-12-30 10:47:38

Dokumentą elektroniniu parašu pasirašė IEVA,KAZLIONKAITĖ
Data: 2020-12-22 21:45:13