INFORMACIJOS SAUGUMO POLITIKA

Taikoma: Visiems Bendrovės darbuotojams ir susijusioms suinteresuotosioms šalims	**Atsakingas už įgyvendinimo koordinavimą:** Kibernetinio saugumo vadovė
Parengė: Kibernetinio saugumo vadovė	**Patvirtino:** Generalinis direktorius
Suderino: Rizikų valdymo vadovas Skaitmeninių technologijų vadovas Kokybės vadovė	

TURINYS

1. BENDROSIOS NUOSTATOS 3
2. TEISĖS AKTAI 4
3. ĮSIPAREIGOJIMAI 5
4. INFORMACIJOS SAUGUMO ORGANIZAVIMAS 5
5. BAIGIAMOSIOS NUOSTATOS 6

1. BENDROSIOS NUOSTATOS

1.1. Informacijos saugumo politika (toliau – Politika) yra pagrindinis AB „Klaipėdos energija“ (toliau – Bendrovė) informacijos saugumo valdymo sistemą (toliau – ISVS) reglamentuojantis dokumentas, skirtas nustatyti Bendrovės informacijos ir kibernetinio saugumo valdymo principus ir efektyvias saugumo užtikrinimo kryptis bei Bendrovės prisiimtus įsipareigojimus, siekiant tinkamai valdyti informacijos ir kibernetinio saugumo rizikas bei užtikrinti tarptautinių ir Lietuvos Respublikos teisės aktų reikalavimų bei Bendrovės prisiimtų įsipareigojimų informacijos ir kibernetinio saugumo srityje įgyvendinimą.

1.2. Politikos tikslas – pateikti Bendrovės vadovybės poziciją informacijos ir kibernetinio saugumo atžvilgiu bei apsaugoti visą Bendrovės informaciją nuo visų galimų grėsmių: išorinių, vidinių, tyčinių ar atsitiktinių, galinčių turėti įtakos Bendrovės vykdomai veiklai ir reputacijai. Informacija – tai strategiškai svarbus Bendrovės veiklai turtas, todėl jos praradimas, neteisėtas pakeitimas, atskleidimas ar informacijos apdorojimo nutraukimas gali sukelti Bendrovės veiklos sutrikimų, padaryti žalos Bendrovei, kitiems fiziniams ir juridiniams asmenims. Atsižvelgiant į tai, Bendrovėje yra keliami ir nustatomi reikalavimai informacijos saugumui.

1.3. Informacijos saugumas apima tris pagrindinius aspektus:

1.3.1. Konfidencialumą – informacijos apsaugą nuo nesankcionuoto atskleidimo;

1.3.2. Vientisumą – informacijos apsaugą nuo nesankcionuoto ar atsitiktinio pakeitimo;

1.3.3. Prieinamumą – užtikrinimą, kad informacija yra prieinama tada, kai ji reikalinga tinkamai vykdyti Bendrovės veiklą.

1.4. Bendrovės informacijos ir kibernetinis saugumas grindžiamas kibernetinio saugumo principais, kurie numatyti Lietuvos Respublikos kibernetinio saugumo įstatymo 3 straipsnyje.

1.5. Politikoje vartojamos sąvokos:

1.5.1. **Atitikties vertinimas** – Bendrovės atitikties Lietuvos Respublikos kibernetinio saugumo įstatymo, Kibernetinio saugumo reikalavimų aprašo, patvirtinto Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“, šios Politikos ir jos įgyvendinimą reglamentuojančių kibernetinio saugumo teisės aktų bei standartų reikalavimams vertinimas;

1.5.2. **Kibernetinio saugumo vadovas** – Bendrovės darbuotojas (arba paslaugas teikianti trečioji šalis), atsakingas už kibernetinio saugumo subjekto atitikties Kibernetinio saugumo įstatymo 14 ir 18 straipsniuose nustatytiems reikalavimams įgyvendinimą ir atliekantis kitas kibernetinį saugumą reglamentuojančiuose teisės aktuose nustatytas funkcijas;

1.5.3. **Rizikos vertinimas** – rizikos vertinimo procesas, apimantis rizikų identifikavimą, jų analizę ir įvertinimą pagal Bendrovės patvirtintą Tinklų ir informacinių sistemų rizikos vertinimo ir valdymo tvarką;

1.5.4. **Saugumo operacijų centras** – Bendrovės generalinio direktoriaus ar jo įgalioto asmens paskirtas asmuo ar grupė, taip pat – paslaugas teikianti trečioji šalis, atsakinga už žurnalinių įrašų ir kibernetinių incidentų stebėjimą ir valdymą;

1.5.5. **Tinklų ir informacinė sistema** (toliau – TIS) – elektroninių ryšių tinklas, bet koks prietaisas arba tarpusavyje sujungtų arba susijusių prietaisų, iš kurių vienas ar daugiau pagal programą automatiškai apdoroja skaitmeninius duomenis, grupė arba skaitmeniniai duomenys, saugomi, tvarkomi, atkuriami arba perduodami nurodytomis priemonėmis jų valdymo, naudojimo, apsaugos ir priežiūros tikslais.

1.6. Kitos šioje Politikoje vartojamos sąvokos suprantamos taip, kaip jos apibrėžiamos Kibernetinio saugumo įstatyme.

1.7. Bendrovės ISVS reikalavimai taikomi:

1.7.1. Visuose Bendrovės veiklos procesuose, susijusiuose su informacijos saugumu bei saugiu informacijos tvarkymu;

1.7.2. Visai Bendrovės informacijai, nepriklausomai nuo jos formos ir saugojimo būdo;

1.7.3. Visoms Bendrovės suinteresuotoms šalims, kurioms teisės aktų ir (ar) sutartinių santykių pagrindu yra suteikta prieiga prie Bendrovės informacinių išteklių teisės aktuose ar sutartyje numatytoms funkcijoms (teisėms) atlikti;

1.7.4. Išorinių paslaugų teikėjų teikiamoms paslaugoms.

2. TEISĖS AKTAI

2.1. Teisės aktai ir standartai, kuriais vadovaujamasi įgyvendinant ISVS:

2.1.1. Kibernetinio saugumo įstatymas;

2.1.2. Lietuvos Respublikos komercinių paslapčių teisinės apsaugos įstatymas;

2.1.3. Lietuvos Respublikos darbo kodekso patvirtinimo, įsigaliojimo ir įgyvendinimo įstatymas;

2.1.4. Lietuvos Respublikos konkurencijos įstatymas;

2.1.5. Lietuvos Respublikos viešųjų pirkimų įstatymas;

2.1.6. Lietuvos Respublikos civilinio kodekso patvirtinimo, įsigaliojimo ir įgyvendinimo įstatymas;

2.1.7. Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimas Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“;

2.1.8. Lietuvos standartas LST ISO/IEC 27001:2022 „Informacijos saugumas, kibernetinis saugumas ir privatumo apsauga. Informacijos saugumo valdymo sistemos. Reikalavimai“ (toliau – Standarto ISO 27001 reikalavimai);

2.1.9. Lietuvos standartas LST ISO/IEC 27002:2022 „Informacijos saugumas, kibernetinis saugumas ir privatumo apsauga. Informacijos saugumo kontrolės priemonės“;

2.1.10. kiti teisės aktai, reglamentuojantys kibernetinį saugumą.

3. ĮSIPAREIGOJIMAI

3.1. Vadovybė įsipareigoja užtikrinti ISVS įgyvendinimą, nuolatinę ISVS plėtrą bei gerinimą.

3.2. Vadovybės funkcijos:

3.2.1. nustatyti Politiką;

3.2.2. nustatyti ISVS tikslus bei patvirtinti ISVS planus;

3.2.3. sudaryti sąlygas Bendrovės darbuotojams tobulinti žinias informacijos saugumo srityje bei informuoti Bendrovės darbuotojus apie atsakomybę už informacijos saugumo pažeidimus;

3.2.4. užtikrinti efektyvų ISVS aprūpinimą reikiamais ištekliais: žmogiškaisiais ištekliais, infrastruktūra (patalpos, aparatinė ir programinė įranga, ryšiai ir kt.), darbo aplinka (tinkamos darbo sąlygos);

3.2.5. numatyti rizikos prisiėmimo ir priimtinų rizikos lygių kriterijus;

3.2.6. užtikrinti reguliarius ISVS vidaus auditus;

3.2.7. atlikti vadovybės vertinamąją ISVS analizę.

3.3. Vadovybė nustato Bendrovės darbuotojams būtiną turėti kvalifikaciją, kuri nurodoma Bendrovės darbuotojų pareigybių aprašymuose.

3.4. Už ISVS veiklų koordinavimą atsakinga vadovybė, kuri užtikrina, kad apie susijusius su ISVS sprendimus būtų informuoti visi su šiais sprendimais susiję Bendrovės darbuotojai.

3.5. Bendrovės darbuotojai Bendrovės nustatyta tvarka privalo būti susipažinę su informacijos saugą reglamentuojančiais teisės aktais ir dalyvauti informacijos saugumo užtikrinimo procese.

3.6. Bendrovės generalinis direktorius ar jo įgaliotas asmuo įsakymu paskiria:

3.6.1. Vadovybės atstovą ISVS;

3.6.2. Kibernetinio saugumo vadovą;

3.6.3. TIS vadovą;

3.6.4. TIS administratorius;

3.6.5. Fizinės saugos įgaliotinį;

3.6.6. Saugumo operacijų centrą;

3.6.7. Veiklos tęstinumo valdymo grupę;

3.6.8. Veiklos atkūrimo grupę.

4. INFORMACIJOS SAUGUMO ORGANIZAVIMAS

4.1. Bendrovėje siekiama šių pagrindinių ISVS tikslų:

4.1.1. apsaugoti visą informaciją nuo visų galimų grėsmių: išorinių, vidinių, tyčinių ar atsitiktinių, galinčių turėti įtakos Bendrovės vykdomai veiklai ir įvaizdžiui;

4.1.2. užtikrinti ir valdyti informacijos saugumą, atsižvelgiant į Bendrovės veiklos strateginius tikslus;

4.1.3. užtikrinti ir valdyti atitikimą išoriniams ir vidiniams informacijos saugumo reikalavimams, atliekant periodinį ISVS vidaus auditą ir atitikties vertinimą bei ISVS valdymo peržiūrą (vadovybės vertinamoji

analizė), šalinant nustatytus trūkumus ir įgyvendinant gerinimo veiksmus;

4.1.4. užtikrinti informacijos saugos incidentų sprendimą, jų priežasčių nustatymą ir pašalinimą, įgyvendinant informacijos saugos incidentų valdymo procesą;

4.1.5. užtikrinti efektyvų rizikos valdymą ir tinkamų rizikos valdymo priemonių naudojimą, siekiant įgyvendinti Rizikų valdymo priemonių planą ir suvaldyti rizikas iki priimtino lygio;

4.1.6. užtikrinti tinkamą informacijos saugumo ir apdorojimo priemonių parinkimą ir įgyvendinimą, atliekant kasmetinį rizikos vertinimą;

4.1.7. užtikrinti reikiamų informacijos saugumo valdymo priemonių įgyvendinimą ir jų veiksmingumą;

4.1.8. užtikrinti veiklos tęstinumo valdymo / atstatymo planų tinkamumą, atliekant jų periodinę peržiūrą ir testavimą;

4.1.9. įgyvendinti TIS2 ir kituose Europos Sąjungos, Lietuvos Respublikos teisės aktuose nustatytus informacijos saugumo reikalavimus, vadovautis Standarto ISO 27001 reikalavimais.

4.2. **Bendrovės ISVS sertifikavimo sritis** „Šilumos (garo ir termofikacinio vandens) gamyba, šilumos perdavimas ir pardavimas Pastatų šildymo ir karšto vandens sistemų priežiūra“.

4.3. ISVS valdymas Bendrovėje yra pagrįstas rizikos valdymu. Informacijos saugumo rizikos vertinimas sudaro sąlygas, kad informacijos ir kibernetinio saugumo valdymo priemonės, taikomos Bendrovės veikloje, atitiktų pagrindinius Bendrovės veiklos bei informacijos ir kibernetinio saugumo tikslus.

4.4. Bendrovės informacijos saugumo rizikų vertinamas atliekamas ne rečiau kaip kartą per metus arba įvykus reikšmingiems Bendrovės pokyčiams, kurie gali turėti poveikį informacijos ir kibernetiniam saugumui.

4.5. Bendrovės ISVS vidaus auditas atliekamas kartu su atitikties vertinimu ne rečiau kaip kartą per metus arba įvykus reikšmingiems Bendrovės pokyčiams, kurie gali turėti poveikį informacijos ir kibernetiniam saugumui. Bendrovėje ne rečiau kaip kartą per 3 metus privalo atlikti atitikties vertinimą nepriklausomi visuotinai pripažintų tarptautinių organizacijų sertifikuoti auditoriai Kibernetinio saugumo įstatymo nustatyta tvarka.

4.6. Bendrovėje vykdomas ISVS procesų ir kontrolės priemonių stebėjimas, matavimai, analizė ir įvertinimas.

4.7. Bendrovėje ne rečiau kaip kartą per metus yra organizuojami arba rengiami veiklos tęstinumo valdymo plano išbandymas bei informacijos ir kibernetinio saugumo mokymai.

4.8. Bendrovėje atliekama vadovybės vertinamoji analizė.

5. BAIGIAMOSIOS NUOSTATOS

5.1. Bendrovės kibernetinio saugumo vadovas reguliariai, ne rečiau kaip kartą per metus arba pasikeitus aplinkybėms, turi peržiūrėti ir, esant poreikiui, atnaujinti Politiką.

5.2. Politika skelbiama Bendrovės interneto svetainėje.

5.3. Politikos privalo laikytis visi Bendrovės darbuotojai ir trečiosios šalys.
5.4. Bet koks ISVS reikalavimų pažeidimas gali daryti neigiamą įtaką Bendrovės veiklos tęstinumui, pakenkti Bendrovės įvaizdžiui visuomenėje ir sukelti teisines pasekmes.
5.5. Bendrovės suinteresuotosioms šalims, pažeidus ISVS reikalavimus, yra taikomos Lietuvos Respublikos įstatymuose, Bendrovės vidaus teisės aktuose bei sutartyse, susitarimuose ar kituose teisinę galią turinčiuose dokumentuose numatytos poveikio priemonės.