PATVIRTINTA
UAB „EPSO-G“
2017 m. rugpjūčio 25d. Valdybos sprendimu
(posėdžio protokolo Nr. VLD-17-15)

UAB „EPSO-G“ ĮMONIŲ GRUPĖS
NESKELBTINOS INFORMACIJOS APSAUGOS POLITIKA

ĮŽANGINĖ DALIS

Neskelbtinos informacijos apsaugos politika skirta sukurti vieningą konfidencialios ir komercinę (gamybos) paslaptį sudarančios informacijos identifikavimo, naudojimo ir apsaugos sistemą.

Ji skirta padėti Grupės bendrovių valdymo organų nariams ir darbuotojams apsaugoti jiems patikėtą konfidencialią informaciją nuo netinkamo ir žalingo atskleidimo.

Politikos nuostatos numato, kad šiam tikslui bendrovėse bus paskirti informacijos apsaugos įgaliotiniai ir/ar administratoriai, kurie kasdieninėje veikloje darbuotojams padės ir patars, kaip darbe užtikrinti informacijos apsaugą ir apsaugoti bendroves nuo galimos žalos. Politikos nuostatos įmonėse bus detalizuojamos atskirose informacijos apsaugos taisyklėse Grupės bendrovės neskelbtinos informacijos apsaugai skirtas priemones diegia vadovaudamosi racionalumo, proporcingumo bei administracinės naštos darbuotojams mažinimo principais.

Tikslas: Užtikrinti EPSO-G įmonių grupėje vieningą ir gerąją praktiką atitinkančią informacijos apsaugą, nustatant informacijos apsaugos principus, sąvokas, vartojamas šioje politikoje ir kituose dokumentuose, nustatančiuose neskelbtinos informacijos apsaugą, informacijos apsaugos valdymo sistemą.

Taikymo apimtis: Taikoma visoms EPSO-G įmonių grupės bendrovėms.

Turinys

1. VARTOJAMOS SĄVOKOS IR SUTRUMPINIMAI

Neskelbtinos informacijos apsaugos politika arba Politika	Ši EPSO-G įmonių grupės neskelbtinos informacijos apsaugos politika su visais priedais, pakeitimais ir papildymais.
EPSO-G	UAB „EPSO-G"
Grupės bendrovės (Bendrovė)	EPSO-G, Dukterinės bendrovės ir Paskesnio lygio dukterinės bendrovės, kaip jos apibrėžtos šiame Politikos skyriuje, ar bet kuri iš šių bendrovių atskirai.
Dukterinės bendrovės (DB)	EPSO-G tiesiogiai kontroliuojamos dukterinės bendrovės.
Paskesnio lygio dukterinės bendrovės (PLDB)	Bendrovės, kurias tiesiogiai ar netiesiogiai kontroliuoja Dukterinės bendrovės.
Informacijos saugumas	Informacijos konfidencialumo, prieinamumo ir vientisumo užtikrinimas.
Konfidencialumas	Informacijos savybė, užtikrinanti duomenų prieinamumą tik tiems vartotojams, kuriems tokia teisė suteikta.
Informacijos saugumo vadybos sistema (ISVS)	Rizikų valdymu pagrįsta įmonės vadybos sistemos dalis, kuria siekiama sukurti, įgyvendinti, valdyti, stebėti, vertinti, prižiūrėti ir gerinti informacijos saugumą. ISVS sudaro: organizacinė struktūra, politika, planavimas, atsakomybė, tvarkos, procesai, procedūros ir ištekliai.
Informacijos saugumo vadovas	Bendrovės vadovui pavaldus ir atskaitingas darbuotojas arba Tretysis asmuo, su kuriuo sudaryta Informacijos saugumo vadovo sutartis, turintis reikiamus įgaliojimus ir resursus Informacijos saugumo vadybos sistemos (ISVS) įgyvendinimui bei atsakingas už jos efektyvumo stebėseną ir tobulinimą.
Informaciniai ištekliai	Informacija (duomenų bazės, duomenų rinkmenos ir dokumentai); programinė įranga (taikomoji ir sisteminė programinė įranga, jos kūrimo priemonės); techninė (aparatinė) įranga (duomenų laikmenos, organizacinė, kompiuterinė ir ryšių įranga); informacinių technologijų ir telekomunikacijų (toliau – ITT) funkcionavimui reikalingos paslaugos; išorės šalių teikiamos ITT paslaugos ir infrastruktūriniai ištekliai; darbuotojų kvalifikacija ir įgūdžiai.
Informacinių išteklių valdytojas (arba administratorius)	Asmuo, Bendrovės vadovo paskirtas atsakingu už informacinių išteklių arba atskirų jų kategorijų (rūšių) saugumą.
Bendrovės informacija	Bet kokios formos Bendrovės valdomi duomenys, neatsižvelgiant į jų fiksavimo ar perdavimo būdą.
Vieša informacija	Bendrovės informacija, kuri yra viešai prieinama, skelbiama arba privalo būti skelbiama teisės aktų nustatytais atvejais ir tvarka (internetinėje svetainėje bendra kontaktinė informacija, veiklos sritys, teikiamos paslaugos, pranešimai žiniasklaidai, Bendrovės naujienos, darbo skelbimai, pranešimai apie konkursus, ir pan.)

Neskelbtina informacija	Bendrovės sukurti ar kitu teisėtu būdu įgyti ir valdomi duomenys, sudarantys Vidinio naudojimo, Konfidencialią informaciją ar Komercinę (gamybos) paslaptį.
Vidinio naudojimo informacija	Bendrovės ir Grupės bendrovių informacija, skirta darbuotojams ir kolegialių organų nariams jų funkcijoms vykdyti ir uždaviniams įgyvendinti, kuri nėra priskirta viešai, konfidencialiai, ar informacijai, sudarančiai komercinę (gamybos) paslaptį ir jos atskleidimas neturėtų neigiamo poveikio Bendrovės veiklai, tačiau dėl savo pobūdžio nėra skirta platinti viešai (pavyzdžiui, detali kontaktinė darbuotojų informacija neskirta skelbti, konfidencialios informacijos neturintys Bendrovės dokumentai, vidinis susirašinėjimas, darbuotojų užimtumo informacija, vidiniai leidiniai ir pan.). Tokio pobūdžio informacija gali būti pažymėta žodžiais „VIDINIO NAUDOJIMO".
Konfidenciali informacija	Bendrovės ir Grupės bendrovių informacija, pažymėta žodžiais „KONFIDENCIALI INFORMACIJA"/„KONFIDENCIALU" *(angl. „Confidential")*, kuriai pagal norminius ir kitus teisės aktus bei Bendrovės sandorius taikomas konfidencialios informacijos statusas. Konfidencialia informacija yra laikoma Bendrovės valdybos patvirtintame konfidencialios informacijos sąraše nurodytų kategorijų informacija, kuri turi tam tikrą ar potencialią vertę Bendrovei dėl to, kad jos nežino Tretieji asmenys ir (ar) kurios atskleidimas gali turėti neigiamą poveikį Bendrovės reputacijai ar finansams.
Komercinė (gamybos) paslaptis	Bendrovės informacija, pažymėta žodžiais „KOMERCINĖ (GAMYBOS) PASLAPTIS" *(angl. „Private and confidential")*, kuri yra Bendrovės valdybos patvirtintame komercinę (gamybos) paslaptį sudarančios informacijos sąraše ir kitų Grupės bendrovių perduota komercinę (gamybos) paslaptį sudaranti informacija. Komercinę (gamybos) paslaptį sudarančia yra laikoma tokia informacija, kuri turi tam tikrą ar potencialią ekonominę vertę Bendrovei dėl to, kad jos nežino Tretieji asmenys, tokia informacija yra itin reta ir (ar) kurios atskleidimas gali sukelti didelę žalą Bendrovės turtiniams ar neturtiniams, bet susijusiems su turtu interesams ar/ir sukelti didelę žalą Bendrovės reputacijai. Informacijos atskleidimas, galintis sukelti didelę turtinę žalą (daugiau kaip 150 MGL dydžio sumą viršijanti žala[1]) visais atvejais turi būti priskiriama komercinę (gamybos) paslaptį sudarančiai informacijai.
Viešai neatskleista informacija	Su EPSO-G įmonių grupe susijęs ir jai žinomas ar privalomas žinoti (įvykęs, numatomas arba planuojamas) įvykis, informacijos apie kurį atskleidimas gali turėti didelį poveikį Grupės bendrovių – emitentų – vertybinių popierių kainai. Esminiais įvykiais gali būti: emitento organų (visuotinio akcininkų susirinkimo, stebėtojų tarybos, valdybos, Bendrovės vadovo) priimti sprendimai; emitento didelės vertės (lyginant su įstatinio kapitalo dydžiu) ilgalaikio turto perleidimo sutarčių sudarymas, nutraukimas, pripažinimas negaliojančiomis, kitoks jų galiojimo pasibaigimas ar vykdymo sustabdymas; stambių sutarčių (prekybinių, kreditinių ir kitų), turinčių ar galinčių turėti esminės įtakos Bendrovės ir Grupės bendrovių veiklai ir finansinei būklei, sudarymas, nutraukimas, pripažinimas negaliojančiomis, kitoks jų galiojimo pasibaigimas ar vykdymo sustabdymas; bet kokie verslo ar veiklos trukdymai, kurie gali turėti reikšmingą poveikį Bendrovės ir Grupės bendrovių finansinei būklei ir pan.
Informacijos atskleidimas	Informacijos perdavimas Trečiajam asmeniui bet kokiu būdu (žodžiu ar raštu) ir priemonėmis (rašytiniuose dokumentuose, kompiuterinėse laikmenose, garso (vaizdo) įrašuose ir pan.) arba sąlygų sudarymas susipažinti su informacija.
Tretieji asmenys	Visi asmenys, kurie nėra EPSO-G ir Grupės bendrovių darbuotojai ar kolegialių organų nariai. Jeigu informacijai neskelbtinos informacijos statusas suteiktas

[1] Lietuvos Respublikos baudžiamojo kodekso 212 str. 1 d. nustatyta, kad XXXI skyriuje „Nusikaltimai ir baudžiamieji nusižengimai ekonomikai ir verslo tvarkai" nurodyta didelė turtinė žala yra 150 MGL dydžio sumą viršijanti žala.

	pagal Bendrovės sudarytą sandorį, trečiaisiais asmenimis laikomi visi asmenys, kurie nėra sandorio šalys ir (ar) jų darbuotojai, kolegialių organų nariai. Trečiaisiais asmenimis nėra laikomos valstybės įgaliotos institucijos, kurios turi teisę gauti tam tikrą informaciją Lietuvos Respublikos teisės aktų nustatytais atvejais ir tvarka.
Sankcionuota įranga	Elektroninės informacijos saugojimo, perdavimo ar apdorojimo aparatinė arba programinė įranga, kurią patvirtino naudojimui Bendrovės vadovas ar jo įgaliotas asmuo.

2. BENDROSIOS NUOSTATOS

2.1. EPSO-G įmonių grupės neskelbtinos informacijos apsaugos politika nustato Neskelbtinos informacijos apsaugos Grupės bendrovėse principus, dokumentuose naudojamas sąvokas, apsaugos organizavimą bei Informacinių išteklių valdymo ypatumus. Politika yra sudedamoji EPSO-G įmonių grupės Informacijos saugumo vadybos sistemos (ISVIS) dalis.

2.2. Politika tvirtinama ir keičiama EPSO-G valdybos sprendimu.

2.3. Politika EPSO-G taikoma tiesiogiai. EPSO-G kolegialūs organai vadovaujasi Politikos nuostatomis tvirtindami EPSO-G dokumentus. EPSO-G siekia, kad su Politika susipažintų ir jos nuostatų laikytųsi visi asmenys, kuriems atskleidžiama arba gali būti atskleista EPSO-G Neskelbtina informacija.

2.4. Rekomenduojama, jog Politika DB ir PLDB būtų įgyvendinama Bendrovių valdyboms priimant sprendimus dėl prisijungimo prie šios Politikos. DB ir PLDB valdyboms priimant sprendimus dėl prisijungimo prie Politikos taip pat rekomenduojama siekti, kad DB ir PLB bendrovių valdysena ir dokumentai, susiję su Neskelbtinos informacijos apsauga atitiktų Politikoje išdėstytus principus bei nustatytas taisykles.

2.5. Už Politikos nuostatų įgyvendinimą, rekomendacijų teikimą Bendrovėms, Politikos aiškinimą (iškilus klausimams), Politikos pateikimą DB ir PLDB informacijos, susijusios su Politikos įgyvendinimu Grupės mastu, surinkimą ir pateikimą EPSO-G valdybai, o taip pat generaliniam direktoriui ne rečiau kaip kartą per metus, yra atsakingas EPSO-G Rizikų valdymo ir prevencijos vadovas.

2.6. EPSO-G šią Politiką skelbia viešai savo interneto tinklapyje. Grupės bendrovėms rekomenduojama skelbti šią politiką viešai pilna apimtimi interneto tinklapyje.

3. NESKELBTINOS INFORMACIJOS VALDYMO PRINCIPAI

Principas „būtina darbui"	Bendrovės konfidencialios, komercinę (gamybos) paslaptį sudarančios informacijos ir (ar) prieigos teisės prie jos Bendrovės darbuotojams, kolegialių organų nariams ir Tretiesiems asmenims gali būti suteikta tik tiek, kiek būtina vykdant konkrečias darbo ir kitas su Bendrove susijusias funkcijas, įsipareigojimus pagal Bendrovės sandorius ar Lietuvos Respublikos teisės aktuose numatytas pareigas ir tik pasirašius konfidencialumo įsipareigojimą.
Atitikties reikalavimams principas	UAB „EPSO-G" valdomos bendrovės, svarbios nacionaliniam saugumui[2], užtikrindamos Neskelbtinos informacijos apsaugą, privalo vadovautis, o kitos Grupės bendrovės turi atsižvelgti į Lietuvos Respublikos energetikos ministro 2013 m. gegužės 2 d. įsakymu Nr. 1-89 „Dėl strateginę ar svarbią reikšmę nacionaliniam saugumui turinčių energetikos ministro valdymo sričiai priskirtų įmonių ir įrenginių informacinės saugos reikalavimų patvirtinimo" nustatytus reikalavimus, o taip pat Lietuvos Respublikos įstatymuose ir kituose norminiuose

[2] Lietuvos Respublikos norminiuose teisės aktuose, reglamentuojančiuose nacionaliniam saugumui svarbių objektų apsaugą, numatytos Bendrovės, kurias kontroliuoja EPSO-G.

	teisės aktuose nustatytus aukščiausius reikalavimus, standartus bei tarptautinę gerąją praktiką.
Neskelbtinos informacijos apsauga turi remtis rizikos valdymo procesu	Nustatoma, kokia Neskelbtina informacija Bendrovėje valdoma; įvertinami informacijos praradimo ir nesankcionuoto atskleidimo tikimybė ir poveikis; planuojamos organizacinės ir techninės priemonės, kurios padėtų sumažinti riziką iki priimtino lygio; informacijos apsaugos politika nuolatos peržiūrima ir atnaujinama.
Veiklos tęstinumo principas	Grupės bendrovėse parengiami veiklos tęstinumo planai, kuriuose numatomas esminių funkcijų ir jų vykdymui būtinos informacijos atkūrimas. Tęstinumo planai turi būti išbandomi, komunikuojami, vykdomi darbuotojų apmokymai.

4. NESKELBTINOS INFORMACIJOS APSAUGOS ORGANIZAVIMAS

4.1. Grupės bendrovės dokumentai turi detaliai apibrėžti Bendrovių vadovų, struktūrinių padalinių vadovų ir darbuotojų teises ir pareigas, kolegialių organų funkcijas, uždavinius ir atsakomybę klasifikuojant informaciją ir užtikrinant Neskelbtinos informacijos apsaugą.

4.2. Grupės bendrovių **valdybos** ir kiti valdymo organai pagal kompetenciją, Bendrovių vadovų teikimu, tvirtina konfidencialią ir komercinę (gamybos) paslaptį sudarančios informacijos sąrašus ir šios informacijos administravimo taisykles.

4.3. Sudarant ir tvirtinant Bendrovės konfidencialios, komercinę (gamybos) paslaptį sudarančios informacijos sąrašus turi būti įvertintos šios informacijos praradimo ir (ar) jos atskleidimo pasekmės:

4.3.1. finansinės – dėl galimų nuostolių Bendrovei;

4.3.2. veiklos – dėl galimų Bendrovės veiklos sutrikimų, apsunkinimų;

4.3.3. teisinės – dėl to, ar praradus arba atskleidus informaciją bus padarytas teisės pažeidimas;

4.3.4. Bendrovės reputacijos sumažėjimo.

4.4. Grupės **bendrovių vadovai** yra atsakingi už Neskelbtinos informacijos apsaugos įgyvendinimą, t. y., tinkamai paskirsto informacijos apsaugai reikalingus išteklius ir reikalavimų įgyvendinimą integruoja į veiklos procesus taip, kad darbuotojams nebūtų didinama administracinė našta.

4.5. Priklausomai nuo Grupės bendrovėje valdomo Neskelbtinos informacijos kiekio, informacijos apsaugos vertinimo, planavimo, įgyvendinimo ir kontrolės funkcijos gali būti:

4.5.1. deleguojamos Informacijos saugumo vadovui (įgaliotiniui);

4.5.2. paskirstomos reikiamą kvalifikaciją turintiems Bendrovės struktūrinių padalinių ar funkciniams vadovams ar darbuotojams;

4.5.3. perduodamos tinkamą kvalifikaciją turintiems tiekėjams pagal Informacijos saugumo vadovo paslaugų teikimo sutartis.

4.6. **Informacijos saugos vadovas (įgaliotinis)** patvirtina ir periodiškai peržiūri visų administratoriaus teises informacinėse sistemose turinčių subjektų sąrašą.

4.7. Apie visus informacijos apsaugos incidentus nedelsiant informuojamas Informacijos saugos vadovas (įgaliotinis). Visi incidentai turi būti registruojami, tinkamai užfiksuojama informacija apie incidentą, pašalinamos pasekmės, mokomasi iš klaidų.

4.8. Nustatytu periodiškumu Informacijos saugumo vadovas (įgaliotinis) parengia ir Grupės bendrovės vadovui pateikia apsaugos incidentų ataskaitą.

4.9. **Struktūrinių padalinių vadovai** yra atsakingi, kad tiesiogiai jiems pavaldūs darbuotojai būtų susipažinę su Neskelbtinos informacijos apsaugos reikalavimais ir nustatyta atsakomybe už jų nesilaikymą.

4.10. Struktūrinių padalinių vadovai inicijuoja prieigos prie informacijos ir dokumentų suteikimą pavaldiems darbuotojams vadovaudamiesi principu „būtina darbui". Organizuojant prieigą prie informacijos elektroniniais tinklais laikomasi principo „draudžiama pagal nutylėjimą" (angl. *default deny*), t. y. draudžiami visi IT protokolai, servisai, funkcijos, programos, išskyrus leistinus.

4.11. Prieigos prie informacijos ir dokumentų inicijavimo ir suteikimo funkcijos turi būti atskirtos.

4.12. Grupės bendrovėse turi būti paskirti darbuotojai atsakingi už dokumentų, kuriuose yra Neskelbtinos informacijos, administravimą ir informacinės saugos administratoriai. Šiems darbuotojams paskiriamos teisės aktuose ir kituose dokumentuose nustatytos **Informacinių išteklių valdytojų** funkcijos.

4.13. Priklausomai nuo Bendrovės valdomo informacinių technologijų ir Neskelbtinos informacijos kiekio ir kritinės įtakos Bendrovei veiklai gali būti sudaryta saugos administratoriaus paslaugų teikimo sutartis.

4.14. Informacinės saugos administratorių teisių naudojimas turi būti griežtai ribojamas ir kontroliuojamas.

4.15. Grupės bendrovėje patvirtintuose dokumentuose (darbo sutartyse, darbo tvarkos taisyklėse, pareiginiuose nuostatuose, konfidencialumo susitarimuose ir kt.) turi būti įtraukti darbuotojams, kolegialių organų nariams ir kitiems asmenims (rangovams, paslaugų teikėjams bei Trečiųjų asmenų atstovams) keliami šie informacijos saugumo reikalavimai, nustatomos prievolės ir atsakomybė:

4.15.1. laikytis Bendrovės Neskelbtinos informacijos apsaugos reikalavimų ir įdiegtų procesų;

4.15.2. įpareigojimas saugoti konfidencialią, komercinę (gamybos) paslaptį sudarančią informaciją turi galioti protingą laiką nutraukus darbo santykius ir (ar) tokios informacijos bei duomenų tvarkymo veiklą, vykdytą sudarytų sutarčių pagrindu.

4.16. Grupės bendrovėje turi būti užtikrinta, kad, nutraukiant darbo santykius su darbuotoju ar sutartį su kolegialaus organo nariu, būtų nedelsiant, bet ne vėliau kaip iki sutarties nutraukimo:

4.16.1. panaikinta prieiga prie informacinių sistemų;

4.16.2. grąžinti visi dokumentai, kuriuose yra Neskelbtinos informacijos;

4.16.3. grąžinta visa Bendrovės suteikta techninė ir programinė įranga.

4.17. Keičiantis darbuotojo, kolegialaus organo nario pareigoms prieiga prie Informacinių išteklių turi būti pakeičiama vadovaujantis principu „būtina darbui".

5. INFORMACINIŲ IŠTEKLIŲ VALDYMO YPATUMAI. INFORMACIJA, DOKUMENTAI

5.1. Grupės bendrovių valdoma **informacija**, esanti visų rūšių fiziniuose dokumentuose, turi būti registruojama nustatyta tvarka.

5.2. Įrenginiuose elektronine forma ir fiziniuose dokumentuose esanti konfidenciali, komercinę (gamybos) paslaptį sudaranti informacija turi būti nustatyta tvarka pažymėta.

5.3. Grupės bendrovėse valdoma informacija yra skirstoma į šias kategorijas:

5.3.1. **Vieša informacija**;

5.3.2. **Neskelbtina** (nevieša) informacija:

5.3.2.1. **Vidinio naudojimo informacija**;

5.3.2.2. **Konfidenciali informacija**;

5.3.2.3. **Komercinę (gamybos) paslaptį** sudaranti informacija.

5.4. Grupės bendrovių, kurių akcijomis prekiaujama reguliuojamoje rinkoje, ir pastarųjų dukterinių bendrovių darbuotojams ir kolegialių organų nariams taikomi reikalavimai[3], nustatyti asmenims, turintiems teisę sužinoti **viešai neatskleistą informaciją**. Tokia informacija yra laikoma tiesiogiai ar netiesiogiai su Grupės bendrovėmis – emitentais[4] – ar jų finansinėmis priemonėmis susijusi tiksli informacija apie planuojamus ar įvykusius esminius įvykius ar kita informacija, kurios viešas atskleidimas gali turėti didelę įtaką Grupės bendrovių, kurių akcijomis prekiaujama reguliuojamoje rinkoje, finansinių priemonių ar su jomis susietų išvestinių finansinių priemonių kainai.

5.5. **Asmens duomenys** turi būti valdomi laikantis šioje Politikoje nustatytų ir Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymo, Lietuvos Respublikos elektroninių ryšių įstatymo ir kitų Europos sąjungos ir Lietuvos Respublikos teisės aktų reikalavimų.

5.6. Grupės bendrovės, ypatingos svarbos informacinės infrastruktūros valdytojai, privalo teikti Nacionaliniam kibernetinio saugumo centrui prie Lietuvos Respublikos krašto apsaugos ministerijos informaciją apie kibernetinius incidentus ir taikytas šių incidentų valdymo priemones, o apie kibernetinius incidentus, susijusius su asmens duomenų apsaugos pažeidimais, ir taikytas šių incidentų valdymo priemones – Valstybinei duomenų apsaugos inspekcijai šios institucijos nustatyta tvarka ir sąlygomis.

5.7. Grupės bendrovėse turi būti diegiama ir palaikoma „švaraus stalo" tvarka, draudžianti palikti be priežiūros dokumentus, bylas, informacijos laikmenas (pvz., darbo kabinete ant stalo pasibaigus darbo laikui), kuriose yra Neskelbtinos informacijos.

5.8. Grupės bendrovėse tiek fiziniai, tiek elektroniniai dokumentai, turi būti tinkamai valdomi ir apsaugoti nuo sugadinimo, praradimo, neteisėto atskleidimo ir naudojimo, pakeitimo ir naikinimo. Turi būti parengta dokumentų valdymo tvarka, kurioje nurodomi pagrindiniai dokumentų rengimo, registravimo, tvarkymo, apskaitos, saugojimo, perdavimo ir naikinimo reikalavimai ir procedūros.

6. INFORMACINIŲ IŠTEKLIŲ VALDYMO YPATUMAI. TECHNINĖ (APARATINĖ), PROGRAMINĖ ĮRANGA IR ELEKTRONINIAI RYŠIAI

6.1. Grupės bendrovių veiklai leidžiama naudoti tik Sankcionuotą įrangą. Informacija gali būti saugoma, apdorojama ir perduodama tik teisėtais pagrindais valdoma (pvz.: nuosavybės teise arba nuomojama) įranga. Tik išimtinais atvejais gali būti leidžiama naudoti kitų asmenų valdomą įrangą (pvz.: kolegialių organų nepriklausomų narių turimi kompiuteriai, mobilieji įrenginiai). Tokie atvejai, kaip ir visa techninė ir programinė įranga turi būti registruojami ir apskaitomi.

6.2. Draudžiama saugoti Bendrovės konfidencialią, komercinę (gamybos) paslaptį sudarančią informaciją Bendrovėje neregistruotuose įrenginiuose ir laikmenose.

6.3. Konfidencialiai, komercinę (gamybos) gamybos paslaptį sudarančiai informacijai saugoti gali būti naudojami tik tokie nešiojami įrenginiai, kuriuose saugoma informacija yra šifruojama.

[3] Lietuvos banko valdybos 2013 m. vasario 28 d. nutarimas Nr. 03-46 „Dėl viešai neatskleistos informacijos konfidencialumo užtikrinimo ir atskleidimo taisyklių patvirtinimo"; 2014 m. balandžio 16 d. Europos Parlamento ir Tarybos reglamentas (ES) Nr. *596/2014* dėl piktnaudžiavimo rinka (Piktnaudžiavimo rinka reglamentas) ir kuriuo panaikinama Europos Parlamento ir Tarybos direktyva 2003/6/EB ir Komisijos direktyvos 2003/124/EB, 2003/125/EB ir 2004/72/EB Tekstas svarbus EEE; 2016 m. kovo 10 d. Komisijos įgyvendinimo reglamentas (ES) *2016/347*, kuriuo pagal Europos Parlamento ir Tarybos reglamentą (ES) Nr. 596/2014 nustatomi techniniai įgyvendinimo standartai, susiję su tiksliu viešai neatskleistos informacijos turinčių asmenų sąrašų formatu ir tų sąrašų atnaujinimu (Tekstas svarbus EEE)

[4] LITGRID AB ir AB „Amber Grid".

6.4. Draudžiama leisti naudoti be priežiūros Tretiesiems asmenims (taip pat ir šeimos nariams ar kitaip susijusiems asmenims) kompiuterinę įrangą, laikmenas, mobiliuosius telefonus ir kitą įrangą, kurioje yra Grupės bendrovės valdomos Neskelbtinos informacijos.

6.5. Prieš perduodant kompiuterinę įrangą remonto darbams iš jos turi būti saugiai pašalinta Neskelbtina informacija.

6.6. Grupės bendrovių dokumentuose turi būti nustatyta pareiga darbuotojams ir kolegialių organų nariams saugoti Bendrovės valdomą kompiuterinę įrangą bei laikmenas, kuriuose yra Bendrovės neskelbtinos informacijos, tiek nuo atsitiktinio praradimo, tiek nuo tyčinio pagrobimo ir pareiga nedelsiant pranešti Bendrovės atsakingam asmeniui apie kompiuterinės įrangos ar laikmenos su Neskelbtina informacija praradimą.

6.7. Nebereikalingos duomenų laikmenos turi būti tinkamai sunaikintos. Draudžiama laikmenas išmesti, parduoti ar kitu būdu perleisti nesunaikintas.

6.8. Bendrovėje turi būti nustatyta duomenų ir laikmenų naikinimo tvarka, taip pat minimalūs reikalavimai patikimam Neskelbtinos informacijos sunaikinimui.

6.9. Grupės bendrovės turi užtikrinti, kad žemiau nurodytus diegimus atliktų ir (arba) sankcionuotų tik įgalioti ir tinkamą kvalifikaciją turintys asmenys:

6.9.1. **programinės** įrangos;

6.9.2. ugniasienių ir antivirusinių sistemų;

6.9.3. operacinės sistemos ir taikomosios programinės įrangos pataisų.

6.10. Įrenginiuose, naudojamuose darbui su Bendrovės informacija, draudžiama keisti operacinės sistemos nustatymus draudžiančius įdiegti programinę įrangą. Leidžiama įdiegti programinę įrangą tik iš patvirtintų tiekėjų.

6.11. Mobiliųjų įrenginių programinė įranga turi būti nuolat atnaujinama gamintojų išleistais papildiniais.

6.12. Informacinėse sistemose turi būti registruojama ir nustatytą laiką išsaugoma saugumo ir kitų įvykių informacija. Informacinių sistemų administratoriams turi būti panaikinta galimybė ištrinti ar redaguoti administratoriaus veiksmų žurnalinius įrašus.

6.13. Grupės bendrovės turi imtis priemonių, apsaugančių nuo bet kokios (lokalios ar nuotolinės) nesankcionuotos **prieigos prie tinklo** paslaugų:

6.13.1. vadovautis principu „draudžiama pagal nutylėjimą" (angl. *default deny*), t. y. draudžiami visi IT protokolai, servisai, funkcijos, programos, išskyrus leistinus;

6.13.2. užtikrinti apsaugą nuo nesankcionuotos loginės ir fizinės prieigos prie kompiuterinio tinklo įrenginių valdymo.

6.14. Grupės bendrovės turi nustatyti reikalavimus interneto ir elektroninio pašto naudojimui. Viešaisiais elektroninių ryšių tinklais perduodamos informacijos Konfidencialumas turi būti užtikrintas naudojant šifravimą, virtualųjį privatų tinklą (angl. *virtual private network*).

6.15. Nustatomi šie draudimai perduoti Konfidencialią, Komercinę (gamybos) paslaptį sudarančią informaciją:

6.15.1. ne Grupės bendrovės suteiktu elektroniniu paštu ar programinėmis priemonėmis;

6.15.2. nešifruotą saugiu būdu viešaisiais tinklais;

6.16. Nustatytu periodiškumu turi būti atliekami:

6.16.1. interneto ir elektroninio pašto naudojimo teisėtumo kontroliniai patikrinimai;

6.16.2. nuolatinis tinklo parametrų ir saugumo įvykių stebėjimas.

6.17. Grupės bendrovėse turi būti nustatytos darbuotojų, kolegialių organų narių prieigos prie informacijos registravimo, ir teisių peržiūros procedūros. Kiekvienas naudotojas turi būti unikaliai identifikuojamas. Suteikiant prieigos prie Bendrovių informacijos teises, turi būti vadovaujamasi principu „būtina darbui".

6.18. Grupės bendrovėse turi būti patvirtinta prisijungimo prie informacinių sistemų, kompiuterinės ir mobiliosios įrangos slaptažodžių naudojimo tvarka. Joje numatomi slaptažodžių suteikimo, panaikinimo, naudojimo ir sudėtingumo reikalavimai. Nesinaudojant sistema nustatytą laiką turi būti automatiškai atsijungiama, įjungiama kompiuterio ekrano užsklanda, apsaugota slaptažodžiu.

6.19. Grupės bendrovės turi nustatyti visų veiklai svarbių duomenų ir programinės įrangos atsarginio kopijavimo ir atkūrimo procesus. Atkūrimas iš atsarginių kopijų turi būti periodiškai išbandomas.

7. INFORMACINIŲ IŠTEKLIŲ VALDYMO YPATUMAI. PERSONALO ŽINIOS IR ĮGŪDŽIAI

7.1. Visi Grupės bendrovių **darbuotojai ir kolegialių organų nariai:**

7.1.1. turi būti supažindinti su konfidencialios, komercinę (gamybos) paslaptį sudarančios informacijos apibrėžimu, sąrašu, saugojimo, perdavimo ir naikinimo reikalavimais ir atsakomybe už jų nesilaikymą;

7.1.2. turi būti informuojami, kad Bendrovė nuolatos stebi ir kontroliuoja, kaip darbuotojai naudoja Informacinius išteklius (valdomą informaciją ir informacines technologijas) ir laikosi nustatytų apsaugos reikalavimų;

7.1.3. turi turėti pakankamas jų funkcijoms atlikti žinias ir įgūdžius apie Neskelbtinos informacijos apsaugą. Grupės bendrovės turi nuolat vertinti šių žinių ir įgūdžių lygį, organizuoti arba atlikti mokymus, teikti informacijos apsaugai aktualią informaciją.