UAB „EPSO-G“ ĮMONIŲ GRUPĖS INFORMACIJOS SAUGOS POLITIKA

TIKSLAS	Nustatyti pagrindinius Grupės Informacijos saugos tikslus, valdymo principus ir atsakomybes, užtikrinant nuolatinį Informacijos saugos vadybos sistemos tinkamumą ir atitiktį Grupės strateginiams tikslams, jos veiksmingumą ir tęstinumą pagal veiklos, teisinius, reguliavimo ir sutartinius reikalavimus.
TAIKYMO APIMTIS	Visoms Grupės bendrovėms

1. Vartojamos sąvokos ir sutrumpinimai

1.1. Šioje politikoje vartojamos sąvokos ar sutrumpinimai turi šias reikšmes:

Bendrovė	UAB „EPSO-G“ (juridinio asmens kodas 302826889), AB „Amber Grid“ (juridinio asmens kodas 303090867), UAB „TETAS“ (juridinio asmens kodas 300513148), Energy cells, UAB (juridinio asmens kodas 305689545), LITGRID AB (juridinio asmens kodas 302564383), BALTPOOL UAB (juridinio asmens kodas 302464881) arba UAB „EPSO-G Invest“ (juridnio asmens kodas 306949519).
Grupės informacija	Bet kokios formos Grupės (bet kurios Bendrovės) valdomi duomenys, neatsižvelgiant į jų fiksavimo ar perdavimo būdą (išsaugota dokumentuose, nuotraukose, kompiuterio diskuose, nešiojamose elektroninėse ir kitose informacijos laikmenose, piešiniuose, brėžiniuose, schemose ir bet kokiose kitose informacijos (duomenų) kaupimo (saugojimo) priemonėse, taip pat ir žodine forma, t. y. egzistuojanti žmogaus atmintyje ir neišsaugota (neišreikšta) jokia materialia forma).
Informacijos sauga	Informacijos konfidencialumo, prieinamumo ir vientisumo bei autentiškumo užtikrinimas.
Informacijos saugos vadybos sistema (ISVS)	Rizikų valdymu pagrįsta, Grupėje taikoma vadybos sistema, kuria siekiama sukurti, įgyvendinti, valdyti, stebėti, vertinti, prižiūrėti ir gerinti Informacijos saugą. ISVS sudaro: organizacinė struktūra, planavimas, atsakomybės, vidaus teisės aktai ir ištekliai. ISVS įgyvendinama visose Bendrovėse ir apima visus jų padalinius, Darbuotojus bei Trečiuosius asmenis, tiek, kiek jie gali daryti įtaką Informacijos saugai.
Informacijos saugos incidentas	Įvykis, dėl kurio kyla pavojus saugomos, perduodamos arba tvarkomos Grupės informacijos, duomenų arba paslaugų, teikiamų arba prieinamų per tinklų ir informacines sistemas, prieinamumui, autentiškumui, vientisumui arba konfidencialumui.

Informaciniai ištekliai	Grupės informacija, programinė įranga, aparatinė įranga, informacinių technologijų ir telekomunikacijų funkcionavimui reikalingos paslaugos ir infrastruktūriniai ištekliai.
Informacinių išteklių valdytojas (savininkas)	Darbuotojas, Politiką įgyvendinančiuose vidaus teisės aktuose nustatyta tvarka Vadovybės paskirtas atsakingu už Informacinių išteklių arba atskirų jų kategorijų (rūšių) saugą, kontroliuojantis prieigą prie šių Informacinių išteklių.
Neskelbtina informacija	Grupės informacija, kuri nepriskiriama Viešai informacijai (pavyzdžiui, vidinio naudojimo, konfidenciali ar komercinę (gamybos) paslaptį sudaranti informacija, viešai neatskleista informacija, asmens duomenys).
Tretieji asmenys	Visi asmenys, kurie nėra Darbuotojai ar Bendrovių kolegialių organų nariai. Trečiaisiais asmenimis taip pat laikomi bet kurioje Bendrovėje praktiką atliekantys asmenys.
Vadovybė	Vadovų grupė, kurią sudaro Bendrovės vadovas ir tiesiogiai Bendrovės vadovui pavaldūs aukščiausio lygmens vadovai.
Vieša informacija	Grupės informacija, kuri yra viešai skelbiama arba gali būti skelbiama teisės aktų nustatytais atvejais ir tvarka (pavyzdžiui, skelbiama bendra kontaktinė informacija, veiklos sritys, teikiamos paslaugos, pranešimai žiniasklaidai, naujienos, darbo skelbimai, viešai paskelbtos ataskaitos ir pranešimai biržoms, pranešimai apie konkursus ir pan.). Vieša informacija taip pat laikomi atviri duomenys, kaip jie apibrėžiami Duomenų atvėrimo tvarkos apraše, patvirtintame Lietuvos Respublikos (toliau – LR) ekonomikos ir inovacijų ministro 2020-12-28 įsakymu Nr. 4-1150 „Dėl Duomenų atvėrimo tvarkos aprašo patvirtinimo”.

1.2. Politikoje taip pat vartojamos sąvokos, kaip jos apibrėžtos UAB „EPSO-G“ įmonių grupės korporatyvinio valdymo politikos priede Nr. 1 „Grupės politikose vartojamų sąvokų sąrašas“.

2. Politikos įgyvendinimo tikslai

2.1. Užtikrinti Grupės informacijos konfidencialumą, vientisumą ir autentiškumą, prieinamumą.

2.2. Vadovaujantis aukščiausiais Informacijos saugos standartais diegti ir vystyti ISVS, užtikrinančią saugią ir patikimą Bendrovių informacinę ir kibernetinę aplinką, prisidedant prie Grupės strateginių tikslų įgyvendinimo..

2.3. Pagal kompetenciją įgyvendinti Nacionalinę kibernetinio saugumo strategiją ir užtikrinti atitiktį taikomiems kibernetinio saugumo reikalavimams.

2.4. Užtikrinti nepertraukiamą Bendrovių veiklą ir atsparumą Informacijos saugos incidentams.

3. Vidaus ir išorės veiksniai

3.1. ISVS vystoma atsižvelgiant į Grupės strategijoje numatytas kryptis bei į Grupės ISVS reikšmingus išorės ir vidaus veiksnius.

3.2. **Grupės ISVS reikšmingi vidaus veiksniai:**

3.2.1. Grupė veiklą vykdo nacionaliniu ir tarptautiniu lygmeniu (įgyvendina nacionaliniam saugumui užtikrinti svarbius projektus, Europinius projektus ir užtikrina atitiktį bendriems reikalavimams);

3.2.2. Bendrovės informacinių sistemų saugumą ir patikimumą užtikrina vertinant ir valdant tiekėjų keliamas rizikas. Grupės energijos perdavimo operatoriai dispečerinio valdymo saugumą ir patikimumą užtikrina nuosavos informacinių technologijų infrastruktūros pagrindu (valdomi ir vystomi ryšiai, duomenų centrai);

3.2.3. Suinteresuotos vidaus šalys yra LR energetikos ministerija, Bendrovių akcininkai, Bendrovės, Vadovybė ir Darbuotojai.

3.3. **Grupės ISVS reikšmingi išorės veiksniai:**

3.3.1. LITGRID AB, AB „Amber Grid“, Energy cells, UAB, pagal LR nacionaliniam saugumui užtikrinti svarbių objektų apsaugos įstatymą valdo nacionaliniam saugumui užtikrinti svarbią reikšmę turinčią infrastruktūrą ir kartu su EPSO-G yra pripažintos antros kategorijos nacionaliniam saugumui užtikrinti svarbiomis įmonėmis, bei vadovaujantis LR kibernetinio saugumo įstatymo nuostatomis yra įtrauktos į esminių Lietuvos kibernetinio saugumo subjektų registrą;

3.3.2. Suinteresuotos išorės šalys yra Nacionalinis kibernetinis saugumo centras, LR krašto apsaugos ministerija, tiekėjai, energetikos įmonės, LR gyventojai, Europos elektros ir dujų perdavimo sistemos operatorių tinklo asociacijos ir kiti partneriai;

3.3.3. Grupė Informacijos saugos srityje veiksmus vykdo bendradarbiaudama ir naudodamasi Nacionalinio kibernetinio saugumo centro teikiamomis paslaugomis, esant konkrečioms aplinkybėms – su Lietuvos policija, bei Valstybine duomenų apsaugos inspekcija.

4. Pagrindiniai Informacijos saugos principai

4.1. **Konfidencialumas** – Neskelbtina informacija yra neprieinama ir nepateikiama leidimo neturintiems asmenims arba automatizuotiems procesams.

4.2. **Vientisumas ir autentiškumas** – Grupės informacija yra saugoma nuo atsitiktinio ar neteisėto pakeitimo, ar sunaikinimo, yra tikra, patikima ir kilusi iš patvirtinto šaltinio.

4.3. **Prieinamumas** – Grupės informacija prieinama, kai jos reikia.

4.4. **Rizikų valdymas** – pagrindas, kuriuo remiasi Grupės Informacijos saugos valdymas, yra nustatomas taikomų priemonių proporcingumas, efektyvumas, nuolatinis tobulinimas. Informacijos saugos rizikų vertinimas atliekamas nuolat, bet ne rečiau kaip kartą per metus arba reikšmingai pasikeitus Bendrovės veiklos pobūdžiui, organizacinei struktūrai, technologinei ar grėsmių aplinkai, įskaitant grėsmių nacionaliniam saugumui vertinimą, teisiniam reguliavimui, taip pat įvykus dideliam kibernetiniam incidentui. Informacijos saugos rizikų valdymo, vertinimo ir analizės metodai taikomi vadovaujantis UAB „EPSO-G“ įmonių grupės rizikų valdymo politika ir metodika, Kibernetinio saugumo įstatymo reikalavimais bei kitais aktualiais teisės aktais.

4.5. **„Būtina darbui“ („būtina žinoti“)** – Neskelbtina informacija ir (ar) prieiga prie jos suteikiama asmenims tik tokia apimtimi, kuri yra būtina vykdant konkrečias darbo ir kitas su Grupe ar Bendrove susijusias funkcijas, įsipareigojimus pagal Bendrovių sandorius ar LR teisės aktuose numatytas pareigas.

4.6. **„Mažiausių teisių prieiga“** – prieiga prie Neskelbtinos informacijos suteikiama mažiausiomis teisėmis (pvz. redagavimo, kopijavimo, persiuntimo ir pan.), kurių pakanka vykdant konkrečias darbo ir kitas su Grupe ar Bendrove susijusias funkcijas, įsipareigojimus pagal Bendrovių sandorius ar LR teisės aktuose numatytas pareigas.

4.7. **Priemonių planavimas ir diegimas koordinuojamas Grupės lygiu** – siekiant identifikuoti bendras Bendrovėms iniciatyvas ir išvengti pasikartojančių funkcijų, administracinių veiklų dubliavimo, išnaudoti Bendrovių stiprybes dalijantis patirtimi ir kompetencijomis.

4.8. **Informacijos saugos priemonės** nustatomos pagal kiekvienos Bendrovės saugos poreikį (pavyzdžiui, rizikos apetitą, vidaus bei išorės veiksnius). Didžiausią Informacijos saugos poreikį turinčiose Bendrovėse taikomos ir diegiamos aukščiausius standartus ir geriausias praktikas atitinkančios kibernetinio saugumo rizikų valdymo priemonės.

4.9. **Informacijos saugos programa** –Bendrovėse taikoma Informacijos saugos veiklos planavimo ir valdymo forma, kuri apima Informacijos saugos rizikų, atitikties bei funkcijos brandos vertinimą, tikslų apibrėžimą ir priemones 3 metų laikotarpiui.

4.10. **ISVS veiklos efektyvumas matuojamas rodikliais** – rodikliai teikiami ir stebimi Grupės lygmeniu, todėl Grupėje naudojami standartizuoti arba vieningus rodiklius užtikrinantys saugos įrankiai ir procesai.

4.11. **ISVS reglamentuojama Grupės lygmeniu** – esminiai Politiką įgyvendinantys vidaus teisės aktai yra valdomi, kuriami ir derinami Grupės lygmeniu. Siekiant, kad Informacijos sauga būtų neatsiejama kasdienės veiklos dalis, prioritetas teikiamas konkrečių Informacijos saugos praktikų integravimui į atitinkamos veiklos vidaus teisės aktus.

4.12. **Kiekvienas Darbuotojas tiesiogiai dalyvauja ISVS įgyvendinime.** Darbuotojams reikalingos žinios suteikiamos vykdant nuolatinius mokymus bei pratybas, priklausomai nuo Darbuotojo atliekamos Informacijos saugos rolės.

5. Atitikties reikalavimai

5.1. Grupėje Informacijos sauga organizuojama laikantis Kibernetinio saugumo įstatyme ir kituose Lietuvos, bei Europos teisės aktuose, Bendrovių sandoriuose numatytų reikalavimų, taikomų Bendrovėms.

5.2. Detalus Informacijos saugą reglamentuojančių teisės aktų sąrašas pateikiamas ir nuolat atnaujinamas UAB „EPSO-G“ įmonių grupės Informacijos saugos tvarkos apraše.

5.3. Informacijos saugos atitiktis patvirtinama vidaus ir išorės auditais, UAB „EPSO-G“ įmonių grupės Informacijos saugos tvarkos apraše numatyta apimtimi ir periodiškumu.

6. Standartų taikymas

6.1. Grupėje Informacijos saugos valdymo kompleksiškumas ir optimalumas užtikrinamas Bendrovėse diegiant ir nuolat tobulinant ISO/IEC 27001 standarto reikalavimus atitinkančią ISVS.

6.2. Aukščiausio Informacijos saugos poreikio Bendrovių ISVS yra patvirtinama galiojančiu ISO/IEC 27001 sertifikatu. Sertifikavimo sritis apima esminius, kiekvienos Bendrovės procesus: LITGRID AB – elektros perdavimo sistemos operatoriaus veikla, AB „Amber Grid” – gamtinių dujų perdavimo operatoriaus veikla, Energy cells, UAB – paskirtojo kaupimo sistemos operatoriaus veikla.

7. Pareigos ir atsakomybės

7.1. EPSO-G valdyba	7.1.1.	Tvirtina šią Politiką, nustato Informacijos saugos užtikrinimo kryptis, tikslus, siekius ir principus Grupėje.
7.2. Vadovybė	7.2.1.	Įsipareigoja diegti veiklos tęstinumą, Informacijos saugos atitiktį ir rizikų suvaldymą užtikrinančias organizacines ir technines priemones, skirti tam būtinus išteklius, siekiant išvengti veiklos sutrikdymo dėl Grupės informacijos vientisumo, autentiškumo, prieinamumo arba konfidencialumo pažeidimo.
	7.2.2.	Kartą per metus susipažįsta su ISVS veiksmingumo Vadovybės ataskaita, ir teikia nurodymus, bei rekomendacijas, siekiant užtikrinti

		ISVS įgyvendinimą, tinkamumą, veiksmingumą ir nuolatinį tobulinimą;
	7.2.3.	Užtikrina, kad už Informacijos saugą atsakingi Darbuotojai turėtų būtinų priemonių, reikalingų pareigoms vykdyti.
7.3. Visų lygių vadovai	7.3.1.	Įgyvendina Informacijos saugos reikalavimus, identifikuoja ir skiria tam būtinus resursus savo padalinio ir (ar) funkcijos, ir (ar) funkcinės srities atsakomybės ribose.
	7.3.2.	Skatina Informacijos saugos kultūrą ir siekia, kad tiesiogiai pavaldūs Darbuotojai būtų susipažinę su Politika ir ją įgyvendinančiais vidaus teisės aktais, suprastų reikalavimus ir rizikas dėl jų nesilaikymo.
7.4. Grupės Informacijos saugos vadovas	7.4.1.	Valdymo konsultacijų teikimo sutarties pagrindu atlieka Grupės kibernetinio saugumo vadovo pareigas ir funkcijas, kaip tai nustatyta Kibernetinio saugumo įstatyme, bei atlieka kitas kibernetinį saugumą reglamentuojančiuose teisės aktuose kibernetinio saugumo vadovui nustatytas funkcijas.
	7.4.2.	Formuoja Informacijos saugos politiką ir vykdo jos įgyvendinimo stebėseną.
	7.4.3.	Rengia ir savo atsakomybės ribose tvirtina Grupės lygmens Informacijos saugos valdysenos dokumentus, vykdo jų peržiūrą.
	7.4.4.	Koordinuoja Informacijos saugos planavimo veiklą tarp Bendrovių.
	7.4.5.	Dalyvauja Grupės Informacijos saugos incidentų ir įvykių valdyme.
7.5. Bendrovių Informacijos saugos vadovai	7.5.1.	Bendrovėse yra paskirti tinklų ir informacinių sistemų (visų) saugos įgaliotiniais ir atlieka saugos įgaliotinių pareigas ir funkcijas, kaip tai nustatyta Kibernetinio saugumo įstatyme. Užtikrina, kad Bendrovė atitiktų Kibernetinio saugumo įstatyme nustatytus reikalavimus, tinkamai valdytų rizikas ir incidentus bei atlieka kitas kibernetinį saugumą reglamentuojančiuose teisės aktuose nustatytas funkcijas.
	7.5.2.	Vertina, planuoja, įgyvendina ir kontroliuoja Informacijos saugą.
	7.5.3.	Įgyvendina Politiką ir organizuoja ją įgyvendinančiuose teisės aktuose numatytų bei rizikas valdančių priemonių diegimą.
	7.5.4.	Rengia ir atnaujina Bendrovės lygmens ISVS dokumentus, veiklos tęstinumo planus bei Grupės Informacijos saugos vadovui teikia Politikos ir ją įgyvendinančių Grupės lygmens vidaus teisės aktų pakeitimų siūlymus.
	7.5.5.	Valdo Informacijos saugos incidentus ir įvykius.
	7.5.6.	Nustato Darbuotojus, turinčius konkretų Informacijos saugumo vaidmenį Bendrovėse, ir užtikrina, kad jų žinios ir įgūdžiai atitiktų jų funkcijai atlikti keliamus reikalavimus bei būtų tinkamai informuoti apie visus pokyčius, reikalingus su vaidmeniu susijusioms atsakomybėms vykdyti.
	7.5.7.	Kiekvienų metų pirmąjį ketvirtį parengia ir Vadovybei pristato su Grupės Informacijos saugos vadovu suderintą ISVS veiksmingumo vadovybės ataskaitą apie: tikslų ir ankstesnėse ISVS peržiūrose identifikuotų veiksmų įgyvendinimą, su ISVS susijusių vidaus ir

		išorės problemų pokyčius, Informacijos saugos veiksmingumą ir tendencijas apie neatitiktis, korekcinius veiksmus, stebėsenos ir matavimo bei audito (jei toks buvo) rezultatus, grįžtamąjį ryšį iš suinteresuotųjų šalių, rizikos vertinimo rezultatus, priemonių plano būklę ir nuolatinio gerinimo galimybes.
7.6. Informacinių išteklių valdytojai (savininkai)	7.6.1.	Priskiria Bendrovės informaciją ir Informacinius išteklius numatytoms saugos klasifikavimo kategorijoms, nustato saugos poreikį bei valdo informacinių išteklių rizikas ir prieigą.
7.7. Darbuotojai	7.7.1.	Laikosi Politikoje ir ją įgyvendinančiuose vidaus teisės aktuose nustatytų reikalavimų.
	7.7.2.	Naudoja Bendrovės suteiktas Informacijos saugos priemones ir savo atsakomybės ribose saugo Bendrovės Informacinius išteklius nuo konfidencialumo, prieinamumo, autentiškumo ir vientisumo pažeidimo (pvz. nesankcionuotos prieigos, atskleidimo, modifikavimo, sunaikinimo).
	7.7.3.	Nedelsdami informuoja Bendrovės ar Grupės Informacijos saugos vadovą apie visus pastebėtus įvykusius ar gresiančius Informacijos saugos incidentus ir Politikos ar kitų vidaus teisės aktų pažeidimus ir kitus Bendrovių padalinius, kaip nustatyta vidaus teisės aktuose.
	7.7.4.	Užtikrina, kad į sutartis su Trečiaisiais asmenimis būtų įtraukti Politiką įgyvendinančiuose dokumentuose numatyti Tretiesiems asmenims taikytini Informacijos saugos reikalavimai bei atsakomybė už jų nesilaikymą.
	7.7.5.	Nacionalinio kibernetinio saugumo centro vadovo ir Bendrovėje nustatyta tvarka išklauso kibernetinio saugumo mokymus, dalyvauja pratybose.

7.8. Detalios Vadovybės, Informacijos saugos vadovų ir kitų Darbuotojų atsakomybės nurodomos Politiką įgyvendinančiuose Grupės vidaus teisės aktuose.

8. Baigiamosios nuostatos

8.1. Politika peržiūrima ir pagal poreikį atnaujinama ne rečiau kaip kartą per metus arba įvykus reikšmingiems pokyčiams (pasikeitus Grupės struktūrai, teisės aktams, įvykus incidentams ar pan.). Ne vėliau kaip per 5 darbo dienas nuo Politikos patvirtinimo ir (ar) pakeitimo dienos, Bendrovių Informacijos saugos vadovai per Nacionalinio kibernetinio saugumo centro informacinę sistemą pateikia dokumento pavadinimą, patvirtinimo datą ir registracijos numerį.

8.2. Supažindinimas su Politika vykdomas Bendrovių vidaus teisės aktuose nustatyta tvarka.