PATVIRTINTA
UAB „Nextury Asset Management“
Valdybos 2020 m. spalio 23 d. sprendimu

VEIKLOS TĘSTINUMO POLITIKA

I. DOKUMENTO PASKIRTIS

1. UAB „Nextury Asset Management“ veiklos tęstinumo politika (toliau – „**Politika**“), parengta vadovaujantis Lietuvos Respublikos informuotiesiems investuotojams skirtų kolektyvinio investavimo subjektų įstatymu (su vėlesniais pakeitimais ir (ar) papildymais), Lietuvos banko valdybos 2012 m. liepos 12 d. nutarimu Nr. 03-144 „Dėl Valdymo įmonių veiklos organizavimo ir vykdymo taisyklių“, Lietuvos banko valdybos 2012 m. liepos 12 d. nutarimu Nr. 03-152 „Dėl valdymo įmonių ir investicinių bendrovių veiklos licencijų išdavimo, keitimo ir jų galiojimo panaikinimo taisyklių patvirtinimo“, taip pat kitais teisės aktais, taikytinais valdymo įmonių veiklai.

2. Veiklos tęstinumo politikos tikslas – užtikrinti, kad tuo atveju, jei sutriktų valdymo įmonės UAB „Nextury Asset Management“ naudojamų sistemų ar procedūrų veikimas, esminiai duomenys būtų išsaugoti, bendrovės funkcijų vykdymas nenutrūktų, o investicinė veikla būtų vykdoma arba, jei tai neįmanoma, per trumpiausią įmanomą laiką duomenys ir funkcijų vykdymas būtų atkurti, o investicinės veiklos vykdymas atnaujintas.

3. Šioje Politikoje numatytos priemonės įsigalioja esant neįprastoms aplinkybėms, dėl kurių Bendrovė gali prarasti įrangą, duomenis ar kitus resursus, reikalingus jos vykdomoms funkcijoms ir teikiamoms paslaugoms užtikrinti, taip pat esant nenumatytoms aplinkybėms, kurios gali neigiamai paveikti Bendrovės valdomų kolektyvinio investavimo subjektų ar jų Investuotojų interesus. Be to, Politika yra taikoma siekiant išvengti ir valdyti rizikas, apibrėžtas Politikos IV skyriuje.

4. Bendrovės veikla laikoma atkurta, jei Bendrovė gali sėkmingai valdyti KIS turtą.

II. SĄVOKOS

5. **Bendrovė** arba **Valdymo įmonė** – UAB „Nextury Asset Management“;

6. **Darbuotojas** – bet kuris UAB „Nextury Asset Management“ darbuotojas (**Darbuotojai** reiškia visus UAB „Nextury Asset Management“ darbuotojus kartu);

7. **Direktorius** arba **Vadovas** – UAB „Nextury Asset Management“ administracijos vadovas;

8. **Investuotojas** – Valdymo įmonės valdomo kolektyvinio investavimo subjekto dalyvis ar potencialus dalyvis;

9. **Kolektyvinio investavimo subjektas** (toliau – „**KIS**“) – investicinis fondas arba investicinė bendrovė, kurių tikslas – platinant investicinius vienetus ar akcijas kaupti asmenų lėšas ir padalijant riziką jas kolektyviai investuoti;

10. **Valdyba** – Valdymo įmonės valdyba;

11. **Priežiūros institucija** – Lietuvos bankas.

III. ORGANIZACINĖS NUOSTATOS

12. Už šios Politikos vykdymą ir Bendrovės veiklos atkūrimą, esant neįprastoms aplinkybėms, yra atsakingas Bendrovės Vadovas.

13. Ši Politika yra saugoma Bendrovės biure, kuriame vykdoma nuolatinė Bendrovės veikla (Gedimino pr. 20-35, Vilnius). Taip pat elektroninė Politikos versija yra saugoma Bendrovės internetinėje duomenų saugykloje tokiu būdu, kad esant poreikiui, atsakingi asmenys galėtų netrukdomai ir operatyviai susipažinti su šia Politika.

14. Esant tokio pobūdžio neįprastoms aplinkybėms, kuomet Bendrovės Vadovas negali dalyvauti užtikrinant Bendrovės veiklos atkūrimą arba yra nepajėgus to padaryti vienas, prie veiklos atkūrimo veiksmų prisideda ir, esant poreikiui, Bendrovės Vadovą pavaduoja bei prie šio plano vykdymo prisideda laikinai einantys Direktoriaus pareigas ar Direktorių pavaduojantys asmenys, o jų nesant - Bendrovės Valdybos pirmininkas, jei reikia ir kiti Darbuotojai.

15. Bendrovės Vadovas dalį funkcijų, atkuriant Bendrovės veiklą, gali perduoti atlikti Darbuotojams, tačiau jis bet kokiu atveju lieka atsakingas už Bendrovės veiklos atkūrimą.

16. Esant tokioms neįprastoms aplinkybėms, kuomet veiklos tęstinumui užtikrinti pati Bendrovė neturi pakankamai resursų, Bendrovės Vadovas gali sudaryti susitarimus ar pirkti paslaugas iš trečiųjų šalių, jei tai padėtų Bendrovei sėkmingai atkurti veiklą.

17. Esant tokio pobūdžio neįprastoms aplinkybėms, kuomet laikinai tenka pakeisti Bendrovės darbo vietą, ar perkelti Bendrovės biurą, alternatyvus Bendrovės biuras yra perkeliamas į kitas Bendrovės Vadovo operatyviai surandamas biuro (arba kitas laikinam darbui tinkamas) patalpas.

18. Iškilus neįprastoms aplinkybėms ir sutrikus Bendrovės veiklai, Bendrovės Vadovas sudaro veiklos tęstinumo valdymo grupę. Šios grupės funkcijos yra sekančios:

    18.1. bendravimas su veiklos atkūrimui samdomais specialistais;

    18.2. bendravimas su teisėsaugos ar kitomis institucijomis;

    18.3. bendravimas su Investuotojais ar jų grupėmis;

    18.4. bendravimas su Darbuotojais ir jų koordinavimas;

    18.5. finansinių ir kitų išteklių, reikalingų Bendrovės veiklai atkurti, įvykus nenumatytai situacijai, paskirstymas ir kontrolė;

    18.6. fizinė turto ir informacijos sauga (kai tai yra būtina);

    18.7. informacinių sistemų veiklos atkūrimas, priežiūra ir koordinavimas;

    18.8. informacinės sistemos duomenų atkūrimo organizavimas;

    18.9. taikomų programų tinkamo veikimo atkūrimo organizavimas;

    18.10. kitos pavestos funkcijos.

IV. PAGRINDINĖS BENDROVĖS VEIKLOJE KYLANČIOS RIZIKOS IR JŲ VALDYMAS

19. *Operacinė rizika* – tai rizika patirti nuostolių dėl netinkamų arba neįgyvendintų Bendrovės vidaus kontrolės procesų, Darbuotojų klaidų ir neteisėtų veiksmų bei informacinių sistemų veiklos sutrikimų arba dėl išorės įvykių įtakos. Pagrindiniai operacinės rizikos šaltiniai: informacinės sistemos (techninės ir programinės įrangos ir kt.); žmogaus įtaka (Bendrovės Darbuotojų ir ne Bendrovės Darbuotojų neteisėti veiksmai); darbo sąlygos (saugių darbo sąlygų pažeidimas ir kt.); klaidos (neteisingų duomenų įvedimas, netinkami teisiniai dokumentai ir kt.). Operacinė rizika yra valdoma šiais būdais: (i) parengiant, įgyvendinant bei reguliariai atnaujinant Bendrovėje atitikties, veiklos organizavimo politikas; (ii) Bendrovėje naudojama apskaitos

sistema (toliau – „**Sistema**“) yra suprogramuota ir veikia taip, kad Sistema besinaudojantis darbuotojas negalėtų atlikti tyčinių ar netyčinių apgaulės veiksmų, pavyzdžiui, sukurti fiktyvių Investuotojų, sudaryti fiktyvių investavimo sutarčių ir panašiai; (iii) užtikrinant, kad Bendrovės veikloje naudojama programinė bei tinklo ir ryšio įranga yra apsaugota nuo programinių virusų, kibernetinių atakų bei kitų nefizinių žalos šaltinių; (iv) užtikrinant, kad elektros energijos laikinas nepasiekiamumas nesukeltų žalos Bendrovės naudojamiems įrenginiams, įrangai ir sistemoms; (v) užtikrinant tinkamą ir saugią darbo aplinką; (vi) visi Bendrovės veikloje naudojami dokumentai yra saugomi tiek fiziniu pavidalu, tiek ir virtualiose laikmenose.

20. *Virtualių duomenų netekimo rizika* – tai rizika, kad Sistemoje saugomi duomenys bus prarasti ar kitaip paveikti, kad nebebūtų galima jų atkurti. Ši rizika valdoma darant visų Sistemos duomenų bei duomenų, kurie yra saugomi kitose sistemose, kopijas.

21. *Fizinio pavojaus rizika* – tai rizika, kad Bendrovės arba trečiųjų šalių, kuriems Bendrovė yra perdavusi vykdyti savo funkcijas, turtui bus padaryta fizinė žala (sužalojant, sunaikinant arba pagrobiant turtą), ir dėl to Bendrovės veikla bus sutrikdyta. Šios rizikos suvaldymas: Bendrovės veiklos vieta (biuras) ar trečiųjų asmenų, kuriems Bendrovė yra perdavusi vykdyti savo funkcijas, veiklos vietos (biurai), yra įrengti saugiuose biurų pastatuose, kur dirba apsaugos darbuotojai, yra įvestos ir veikiančios apsaugos sistemos (pvz., signalizacija), tinkamai veikiančios priešgaisrinės sistemos.

22. *Licencijos netekimo rizika* – tai rizika, kad Bendrovė neteks veiklos leidimo valdyti informuotiesiems investuotojams skirtų kolektyvinio investavimo subjektų (toliau - „**Licencija**“) – ir dėl to Bendrovė nebegalės tinkamai vykdyti sutarčių su Investuotojais, investavusiais į Bendrovės valdomus KIS. Licencijos netekimo rizika valdoma šiais būdais: (i) Bendrovės veikla yra prižiūrima Priežiūros institucijos, kas užtikrina savalaikį galimų veiklos neatitikimų teisės aktams pastebėjimą bei užkerta kelią tolimesniems pažeidimams; (ii) Bendrovė, būdama finansų įstaiga, pasibaigus kiekvieniems finansiniams metams, atlieka išorės auditą, o finansinių metų eigoje atlieka įvairius veiklos patikrinimus (pvz., teisinius), kurių metu yra nustatomos ir įvertinamos Bendrovės veikloje kylančios rizikos ir priemonės, padedančios jas suvaldyti; (iii) Bendrovė samdosi išorės konsultantus, kurie nuolatos peržiūri tiek Bendrovės, tiek jos valdomų KIS veiklos dokumentus, teikia konsultacijas Bendrovės veiklos klausimais ir pan., taip užtikrinant savalaikę Bendrovės veiklos kontrolę.

23. *Likvidumo rizika* – tai rizika, kad Bendrovė nesugebės laiku įvykdyti finansinių įsipareigojimų, pasireiškianti laikinu arba nuolatiniu Bendrovės nemokumu ir kraštutiniu atveju – bankroto bylos Bendrovei iškėlimu. Likvidumo rizika valdoma: Bendrovė, turėdama Licenciją, yra atskaitinga Priežiūros institucijai ir teisės aktų nustatyta tvarka nuolatos teikia duomenis apie Bendrovės finansinę būklę Priežiūros institucijai, kas užtikrina tinkamą Bendrovės išorės priežiūrą.

24. *Valdymo rizika* – tai rizika, kad dėl netinkamo Bendrovės ar atskirų jos vykdomų projektų valdymo Bendrovei ar tretiesiems asmenims bus padaryta žala. Valdymo rizika yra valdoma šiais būdais: (i) Bendrovės įstatuose numatyta dviejų pakopų valdymo sistema. Veikia šie valdymo organai: Valdyba ir Vadovas. Bet kuriam vienam iš valdymo organų neatliekant jam teisės aktais bei Bendrovės įstatais priskirtų funkcijų, šios funkcijos atlikimą gali perimti kitas organas. Jei atitinkamos funkcijos perėmimas nėra leidžiamas teisės aktų, Valdyba apie tai informuojama ir teikia pasiūlymą visuotiniam akcininkų susirinkimui. Tokia valdymo sistema užtikrina, kad visos teisės aktų nustatytos funkcijos būtų atliekamos tinkamai ir laiku; (ii) Bendrovės valdymo organų narių kandidatūros iš anksto (prieš šiuos asmenis paskiriant į atitinkamas pareigas) yra patvirtinamos Priežiūros institucijos.

25. *Reputacijos rizika* – tai rizika, galinti neigiamai paveikti Bendrovės pajamas ir kapitalą dėl nepalankios nuomonės apie Bendrovės reputaciją, kurią susidaro klientai, sandorio šalys, investuotojai. Reputacijos rizika valdoma užtikrinant tinkamą Bendrovės valdymą bei bendradarbiaujant su išorės konsultantais, padedančiais valdyti ir kurti teigiamą Bendrovės reputaciją.

V. BENDROVĖS VEIKLAI KELIANČIOS PAVOJŲ APLINKYBĖS IR JŲ PREVENCIJOS PRIEMONĖS

26. Bendrovės Vadovas privalo pasirūpinti, kad būtų užtikrinamos šios sąlygos:

26.1. laiku identifikuojamos grėsmės, galinčios sukelti neįprastas aplinkybes;

26.2. vertinama neįprastų aplinkybių atsiradimo rizika;

26.3. nustatomi aiškūs ir objektyvūs kriterijai, kurie identifikuotų grėsmę keliančių neįprastų aplinkybių atsiradimo pradžią;

26.4. iš anksto nustatomos neįprastų aplinkybių galimos pasekmės Bendrovei, Bendrovės valdomiems KIS bei Investuotojams;

26.5. ne rečiau kaip kartą per metus būtų peržiūrimas ir, esant reikalui, atnaujinamas neįprastas aplinkybes galinčių sukelti grėsmių sąrašas.

27. Pagrindiniai veiksniai, galintys daryti įtaką Bendrovės veiklos sutrikimams, yra šie:

27.1. Bendrovės specialistų laikinas nedarbingumas ar tam tikrų žinių susikoncentravimas pas konkretų Darbuotoją. Šios grėsmės prevencinės priemonės yra sekančios:

27.1.1. Darbuotojai turi dalintis informacija apie einamuosius darbus per vykdomus savaitinius einamųjų darbų aptarimo susirinkimus;

27.1.2. esant galimybei Darbuotojas privalo trumpai aprašyti ir perduoti einamuosius darbus savo kolegai;

27.1.3. esant galimybei ir būtinumui, Darbuotojai turi bendrauti telefonu ar el. paštu, kuomet atliekami perduoti darbai;

27.1.4. Bendrovės veikloje naudojami finansiniai modeliai bei turto valdymo strategijos turi būti aprašytos bei pastoviai atnaujinamos. Aprašymus saugo Bendrovės Vadovas;

27.1.5. Darbuotojai savo veikloje naudojamus duomenis (dokumentus, kontaktus ir pan.) privalo periodiškai įrašyti išorinėje duomenų saugykloje, kuri saugoma pas Bendrovės Vadovą;

27.1.6. esant finansinėms galimybėms, Bendrovė turėtų plėsti personalą taip siekiant kuo mažiau funkcijų koncentruoti pas vieną konkretų Darbuotoją.

27.2. Bendrovėje atsiradę finansiniai sunkumai. Šios grėsmės prevencinės priemonės yra sekančios:

27.2.1. Bendrovės Vadovas kontroliuoja, kad apmokėjimų vėlavimas už Bendrovės suteiktas paslaugas neviršytų 30 (trisdešimt) dienų termino;

27.2.2. Bendrovės Vadovas turi užtikrinti, kad Bendrovė visada turėtų lėšų rezervą, kurio užtektų 3 (trijų) mėnesių einamiesiems įsipareigojimams padengti;

27.2.3. Bendrovės valdomų KIS lėšos yra atskirtos nuo Bendrovės lėšų. KIS lėšos bei finansinės priemonės yra saugomos pas turto saugotoją / depozitoriumą;

27.2.4. Bendrovės finansinės ataskaitos ne rečiau nei kas ketvirtį pateikiamos akcininkams, taip siekiant didesnės finansų kontrolės ir pasiruošimo galimam kapitalo didinimui (jei jo prireiktų).

27.3. Svarbių Bendrovės veikloje naudojamų elektroninių dokumentų ar modelių praradimas. Šios grėsmės prevencinės priemonės yra sekančios:

27.3.1. visi elektroniniai dokumentai, kurie yra naudojami Investuotojams teikiant Bendrovės paslaugas, bei elektroniniai dokumentai, kuriuose saugoma informacija apie Investuotojus, KIS dokumentai, taip pat ir kiti Bendrovės veiklai svarbūs elektroniniai dokumentai (modeliai), yra ne rečiau kaip kartą į mėnesį išsaugomi Microsoft Data serveryje bei Bendrovės internetinėje duomenų saugykloje;

27.3.2. Bendrovės valdomų KIS apskaitos dokumentai Microsoft Data serveryje yra išsaugomi ne rečiau kaip kartą per savaitę;

27.3.3. Microsoft Data serveris turi būti apsaugotas slaptažodžiu;

27.3.4. visi kiti Bendrovės elektroniniu būdu parengti dokumentai bei sutartys taip pat turi būti išsaugoti ir originalioje elektroninėje versijoje;

27.3.5. visuose Bendrovės naudojamuose kompiuteriuose turi būti įdiegta antivirusinė programa, naudojama „ugniasienė“ (angl. *firewall*) bei kitos pagal Bendrovės veiklos pobūdį būtinos saugumo priemonės;

27.3.6. Darbuotojai, jų nuomone, svarbius bei Bendrovės veiklai būtinus dokumentus, gali išsaugoti Bendrovės internetinėje duomenų saugykloje „debesyje“ (angl. *cloud*);

27.3.7. prieiga prie Bendrovės darbuotojų personalinių kompiuterių apsaugota slaptažodžiu;

27.3.8. visuose personaliniuose kompiuteriuose yra naudojama ir reguliariai atnaujinama antivirusinė programa;

27.3.9. visuose personaliniuose kompiuteriuose yra naudojama tik legali programinė įranga.

27.4. Bendrovės organizacinės technikos (IT) gedimai, kuomet nebeįmanoma naudotis kompiuteriais. Šios grėsmės prevencinės priemonės yra sekančios:

27.4.1. išmanieji mobilieji telefonai. Nebeveikiant Bendrovės kompiuteriams ar interneto ryšiui, išmanieji mobilieji telefonai su interneto prieiga būtų laikinai naudojami kaip alternatyva kompiuteriams, informacijos gavimui ir elektroninei komunikacijai (elektroniniai laiškai ir pan.);

27.4.2. pakaitiniai kompiuteriai. Sugedus Bendrovės kompiuteriams, laikinai galima naudotis Darbuotojų asmeniniais kompiuteriais, į juos perkeliant reikalingus duomenis iš išorinio duomenų kaupiklio ar internetinės duomenų saugyklos;

27.4.3. siekiant užtikrinti, kad Bendrovė galėtų nepertraukiamai aptarnauti Investuotojus, bus naudojami iš anksto paruošti dokumentai arba dokumentų šablonai, kuriuos bus galima užpildyti ranka įrašant reikiamus duomenis. Bendrovėje visuomet privalo būti atspausdinta bent po keletą egzempliorių šių dokumentų:

27.4.4. Bendrovės patvirtintų finansinių priemonių pobūdžio bei joms būdingos rizikos aprašymų;

27.4.5. Bendrovės patvirtintos interesų konfliktų vengimo politikos;

27.4.6. Investuotojų investuojant pildomi klausimynai;

27.4.7. skundo ar prašymo priėmimo formų;

27.4.8. Bendrovės valdomų KIS prospektų aprašymai;

27.4.9. KIS vienetų pardavimo bei išpirkimo sutarčių (paraiškų);

27.4.10. KIS veiklos ataskaitų.

27.5. Finansų rinkos dalyvių bankrotai, banko bankrotas ir pan. Šios grėsmės prevencinės priemonės yra sekančios:

27.5.1. Bendrovė turi atsidariusi sąskaitą viename didžiausių Lietuvoje veikiančių komercinių bankų;

27.5.2. Bendrovė nuolatos stebi ir vertina bankų, kuriuose laikomos Bendrovės lėšos finansinę būklę ir bankų kapitalo pakankamumo rodiklius.

27.6. Bendrovėje saugomų dokumentų, kompiuterių ar kitų Bendrovės veikloje naudojamų priemonių vagystė arba netekimas gaisro atveju. Šios grėsmės prevencinės priemonės yra sekančios:

27.6.1. patekimas į pastatą, kuriame įsikūrusi Bendrovė, ne nustatytomis darbo valandomis yra leidžiamas tik asmenims, turintiems identifikacines korteles;

27.6.2. patekimas į Bendrovės patalpas ne nustatytu darbo metu galimas tik įvedus atskirą patalpų apsaugos signalizacijos slaptažodį;

27.6.3. patalpų, kuriose įsikūrusi Bendrovė, signalizacija yra sujungta su bendra pastato signalizacija. Signalizacijos stebėseną atlieka apsaugos tarnyba;

27.6.4. patalpose, kuriose įsikūrusi Bendrovė, yra įrengta priešgaisrinė signalizacija, sujungta su pastato priešgaisrine signalizacija;

27.6.5. patalpos atitinka priešgaisrinės saugos reikalavimus, jose yra gaisro gesinimo priemonės. Periodiškai atliekama gaisro gesinimo priemonių patikra;

27.6.6. visi svarbiausi Bendrovėje naudojami dokumentai (tame tarpe sutartys, paraiškos ir pan.) yra nuskenuojami ir periodiškai perkeliami į ne Bendrovės biure esančias duomenų saugyklas.

27.7. Bendrovės veiklos sutrikimai dėl elektros tiekimo laikino arba ilgalaikio nutrūkimo. Šios grėsmės prevencinės priemonės yra sekančios:

27.7.1. Bendrovės veikloje siekiama naudoti sąlyginai naujus nešiojamuosius kompiuterius. Šių kompiuterių darbo laikas be papildomo elektros šaltinio (naudojant tik kompiuterio bateriją) siekia 5 – 9 valandas. Atsižvelgiant į Bendrovės veiklos pobūdį, 5 – 9 valandų termino visiškai pakanka, kad būtų atlikti skubūs ar būtinieji darbai: sandorių atlikimas, Fondo paraiškų vykdymas, GAV skaičiavimas, Fondo vertės paskelbimas ir pan.;

27.7.2. esant ilgesniems elektros tiekimo sutrikimams, nešiojamieji kompiuteriai lengvai perkeliami į alternatyvią darbo vietą, kur būtų užtikrintas elektros tiekimas;

27.7.3. elektros tiekimo sutrikimo atveju, prie interneto galima prisijungti naudojantis Bendrovės išmaniusiuose telefonuose esančiais bevieliais modemais.

VI. PASIRENGIMAS NEĮPRASTŲ APLINKYBIŲ VALDYMUI

28. Esant situacijai, kai grėsmes Bendrovės veiklai sukeliančių neįprastų aplinkybių neįmanoma nedelsiant likviduoti, Bendrovėje turi būti parengiamas tokios situacijos likvidavimo planas. Likvidavimo planą parengia Bendrovės Vadovas, jis turi būti patvirtintas Bendrovės Valdybos.

29. Neįprastų aplinkybių likvidavimo planuose turi būti nurodoma:

29.1. Bendrovei, KIS ar Investuotojų interesams kylančios grėsmės pobūdis;

29.2. kriterijai, pagal kuriuos galima nustatyti, jog atsirado neįprastos aplinkybės;

29.3. neįprastų aplinkybių galimos pasekmės Bendrovei, KIS ar Investuotojų interesams;

29.4. veiksmų seka, kurių reikia imtis likviduojant neįprastas aplinkybes;

29.5. už konkrečių neįprastų aplinkybių suvaldymą ir likvidavimą atsakingi asmenys.

30. Bendrovėje turi nuolatos būti visi reikalingi resursai bei priemonės, būtini neįprastų aplinkybių sukeltų padarinių pašalinimui bei prevencijai.

VII. NEĮPRASTŲ APLINKYBIŲ LIKVIDAVIMAS

31. Atsižvelgiant į Investuotojų interesus, neįprastų aplinkybių atsiradimo atvejais Bendrovės veikla atkuriama pagal Bendrovės vykdomų veiklų prioritetą tokia eilės tvarka:

31.1. pagrindinė veikla, t. y. Bendrovės valdomų KIS turto apsauga bei valdymas (šių funkcijų vykdymas turi būti užtikrintas ir neįprastų aplinkybių metu);

31.2. svarbi veikla, t. y. Investuotojų turimų investicinių vienetų ar akcijų išpirkimas ir atsiskaitymas su jais bei investicinių vienetų ar akcijų pardavimas Investuotojams;

31.3. kita įprastinė Bendrovės veikla.

32. Konkretūs veiksmai, kurių turi būti imamasi likviduojant neįprastas aplinkybes, privalo būti nurodyti jų likvidavimo planuose.

33. Neįprastų aplinkybių likvidavimo procesas turi būti organizuojamas atsižvelgiant į žemiau pateiktas gaires:

33.1. apie neįprastų aplinkybių Bendrovėje atsiradimą informuojamas Bendrovės Valdybos pirmininkas bei, pagal poreikį, teisėsaugos, draudimo, priežiūros bei kitos institucijos;

33.2. pirmiausia turi būti atliekami veiksmai tęsiant pagrindinę Bendrovės veiklą bei užtikrinamas nenutrūkstamas ir pilnas pagrindinės veiklos funkcionavimas;

33.3. pasirūpinama resursais, reikalingais pagrindinės veiklos vykdymui (darbo vietos, kompiuteriai, jų tinklas, ryšio priemonės, prieiga prie interneto). Jei yra būtinybė, užsakomos pagrindinės veiklos vykdymui reikalingos paslaugos iš trečiųjų šalių;

33.4. užtikrinant pagrindinės veiklos funkcionavimą, gali būti priimami laikini sprendimai, kurie nustoja galioti pilnai likvidavus neįprastas aplinkybes;

33.5. užtikrinus pagrindinės veiklos funkcijas, imamasi priemonių svarbiai Bendrovės veiklai atkurti;

33.6. pilnai atkūrus visas Bendrovės veiklas, patvirtinamos ilgalaikės priemonės (sprendimai), kurios pakeičia laikinas priemones, naudotas neįprastų aplinkybių metu;

33.7. neįprastų aplinkybių likvidavimo plane taip pat turi būti nurodoma, kam ir kokia informacija turi / gali būti pateikiama apie situaciją Bendrovėje.

34. Tokiais atvejais, kai Bendrovėje nėra parengtas konkrečios situacijos neįprastų aplinkybių likvidavimo planas, Bendrovės Vadovas privalo operatyviai priimti reikiamus sprendimus bei duoti nurodymus Darbuotojams, kad neįprastos aplinkybės būtų kuo skubiau likviduotos.

VIII. BAIGIAMOSIOS NUOSTATOS

35. Ši Politika įsigalioja nuo jos patvirtinimo ir visa apimtimi galioja iki jos pakeitimo, papildymo ar panaikinimo.

36. Ši Politika gali būti keičiama ir (ar) papildoma tik Bendrovės Valdybos sprendimu.

37. Už Politikos įgyvendinimą, priežiūrą, atnaujinimą ir laikymosi kontrolę yra atsakingas Bendrovės Vadovas.

38. Su šia Politika Darbuotojai yra supažindinami pasirašytinai.

39. Bendrovės Vadovas, vadovaudamasis šia Politika, bent kartą per metus privalo atlikti Bendrovės veiklos tęstinumą užtikrinančių informacinių technologijų priemonių testavimą. Atlikus testavimą ir išaiškėjus naujoms aplinkybėms, Politika turi būti atnaujinama taip, kad būtų užtikrintas Bendrovės veiklos tęstinumas atsižvelgiant į naujas aplinkybes.