UAB „OZ FINANCE“
VEIKLOS TĘSTINUMO PLANAS

1. BENDROSIOS NUOSTATOS

1.1. Šis UAB „Oz Finance“ („**Bendrovė**“) veiklos tęstinumo planas („**Planas**“) nustato taikomas priemones bei procedūras, užtikrinančias, kad:

1.1.1. Bendrovės įsipareigojimų nevykdymo atveju būtų toliau teikiamos Ypatingos svarbos paslaugos, susijusios su atliktomis investicijomis į sutelktinio finansavimo projektus;

1.1.2. būtų tinkamai administruojami Bendrovės ir Bendrovės klientų susitarimai;

1.1.3. ekstremalių situacijų atvejais Bendrovės veikla būtų nepertraukiama;

1.1.4. būtų apribojami bet kokio pobūdžio nuostolius Bendrovės veiklos sutrikimų atvejais.

1.2. Šis Planas yra parengtas pagal Bendrovės teikiamų paslaugų pobūdį, mastą bei sudėtingumą. Už Plano įgyvendinimą Bendrovės veikloje yra atsakingas Bendrovės vadovas. Tuo atveju, jeigu Bendrovės dėl tam tikrų objektyvių priežasčių (pvz., vadovas yra išvykęs) negali atlikti savo funkcijų, Bendrovės vadovas iš anksto turi paskirti Bendrovės darbuotoją visų šiame Plane numatytų Bendrovės priskirtų funkcijų atlikimui

2. PLANE VARTOJAMOS SĄVOKOS

2.1. Šiame Plane vartojamos sąvokos turi žemiau nurodomas reikšmes:

2.1.1. **Bendrovė** – UAB „Oz Finance“, juridinio asmens kodas 304962927, buveinė registruota adresu Ašigalio g. 1B, Kaunas, Lietuva;

2.1.2. **Finansuotojas** – investavimo pasiūlymą per Platformą pateikęs fizinis asmuo arba juridinis asmuo, kuris tinkamai užsiregistravo Platformoje;

2.1.3. **Ypatingos svarbos paslaugos** – Bendrovės operacinės ir verslo paslaugos, kurių sutrikimas ar netinkamas veikimas iš esmės trukdytų Bendrovės nuolatiniam reikalavimų ir įsipareigojimų laikymuisi pagal Reglamentą, pakenktų Bendrovės finansiniams rezultatams arba Bendrovės teikiamoms sutelktinio finansavimo paslaugoms, Bendrovės veiklos patikimumui ar tęstinumą, ypač Klientų atžvilgiu;

2.1.4. **Klientas** – Projekto savininkas arba Investuotojas;

2.1.5. **Planas** – šis veiklos tęstinumo planas;

2.1.6. **Platforma** – Bendrovės operuojama sutelktinio finansavimo platforma „Oz Finance“;

2.1.7. **Priežiūros institucija** – Lietuvos bankas;

2.1.8. **Projektas –** verslo, profesinėms, mokslo, tiriamosioms ir kitoms reikmėms, išskyrus vartojimą, tenkinti parengtas ir Platformoje paskelbtas Projektas, kuriam įgyvendinti Projekto savininkas iš Investuotojų siekia pritraukti sutelktinio finansavimas lėšas;

2.1.9. **Projekto savininkas** – asmuo, inicijuojantis verslo, profesinėms, mokslo, tiriamosioms ir kitoms reikmėms, išskyrus vartojimą, tenkinti skirtą ir Platformoje skelbiamą Projektą, kuriam įgyvendinti yra reikalingos Investuotojų sutelktinio finansavimo lėšos;

2.1.10. **Reglamentas** – Reglamentas (EU) 2020/1503.

2.2. Kitos šiame Plane naudojamos sąvokos suprantamos taip, kaip jos apibrėžtos Reglamente. Jei kontekstas nereikalauja kitaip, Politikoje žodžiai vartojami vienaskaita apima ir daugiskaita vartojamus žodžius, ir atvirkščiai.

3. RIZIKŲ ANALIZĖ

3.1. Bendrovė savo veiklos tęstinumą planuoja atsižvelgdama vertinant bei analizuojant galimą poveikį Bendrovės veiklai. Bet kokie Bendrovės veiklos sutrikimai visais atvejais yra vertinami atsižvelgiant į:

3.1.1. finansinį poveikį Bendrovei;

3.1.2. poveikį Bendrovės veiklai ir/ar teikiamoms paslaugoms;

3.1.3. finansinį poreikį, reikalingą Bendrovės veiklos ir/ar teikiamų paslaugų atkūrimui ir tęstinumo užtikrinimui po atitinkamos veiklos ir/ar atskiros funkcijos sutrikimo;

3.1.4. esamą Bendrovės pasiruošimą veikti nenumatytomis aplinkybėmis;

3.1.5. Bendrovės veiklai vykdyti būtinas informacines ir ryšių technologijas.

3.2. Bendrovė, siekdama užtikrinti nenutrūkstamą savo veiklą, atsižvelgia į rizikas, su kuriomis gali susidurti savo veiklos metu. Šios rizikos apima, tačiau neapsiriboja šiais scenarijais:

3.2.1. Bendrovės patalpų praradimas;

3.2.2. Bendrovės darbuotojų negalėjimas vykdyti savo funkcijų;

3.2.3. techninės įrangos gedimai;

3.2.4. Platformos sutrikimai;

3.2.5. Duomenų praradimas;

3.2.6. mokėjimo ir tapatybės nustatymo paslaugų teikėjų veiklos sutrikimai;

3.2.7. kibernetinės atakos

3.3. Siekiant užtikrinti Bendrovės veiklos tęstinumą, Bendrovės vadovas periodiškai, tačiau ne rečiau kaip kartą per metus, atsižvelgdamas į Bendrovės teikiamų paslaugų pobūdį, mastą ir sudėtingumą, analizuoja aplinkybes ir situacijas, susijusias su Bendrovės operacinės rizikos atsiradimu, jų tikimybe.

3.4. Plane numatytos atkūrimo priemonės ir prevencinės priemonės atitinka galimos rizikos atsiradimo tikimybę ir jos poveikį Bendrovės veiklai, vertinant jas pagal tris lygius: žemą, vidutinį ir aukštą.

3.5. Bendrovė nustatė šias pagrindines funkcijas, kurioms būtinas nepertraukiamas veiklos tęstinumo užtikrinimas

	Funkcija	**Galimas poveikis Bendrovės veiklai**
1.	Pagrindinės informacijos (tokios kaip turimos paskolos, suteikti finansavimai, mokėjimo terminai ir kt.) Klientų paskyrose Platformoje	Žemas
2.	Klientų prisijungimas bei naudojimasis paskyra Platformoje	Vidutinis
3.	Nepertraukiamas informacijos apie Bendrovės Klientus ir jų atliktas operacijas registravimas ir saugojimas	Vidutinis
4.	Bendrovės ūkinės veiklos operacijų valdymas	Vidutinis
5.	Pagrindinių operacijų vykdymas platformoje (finansavimai bei finansavimų gavimai Projektams)	Aukštas
6.	Bendrovės Klientų identifikavimas bei tapatybės nustatymas	Aukštas

3.6. Atsižvelgiant į rizikų analizę, Bendrovė dės pastangas, kad būtų užtikrinamos procedūros, kuriomis būtų siekiama užtikrinti komunikacijos tarp Bendrovės ir Klientų, Bendrovės verslo partnerių, darbuotojų ir Priežiūros institucijos tęstinumą.

4. BENDROVĖS VEIKLOS ATSTATYMAS BENDROVĖS PATALPŲ PRARADIMO ATVEJU

4.1. Bendrovės patalpų praradimo atveju (pvz., kylant gaisrui, kariniam konfliktui, stichinei nelaimei, teroro aktui, nusikalstamų veikų ar kt.), visų pirma, užtikrinama, kad būtų vykdoma Bendrovės darbuotojų bei kitų Bendrovės patalpose esančių asmenų evakuacija.

4.2. Bendrovės vadovas ar jo įgaliotas asmuo:

4.2.1. priima sprendimą dėl tolimesnių veiksmų, reikalingų veiklos procesams tęsti;

4.2.2. imasi priemonių siekiant išvengti Bendrovės dokumentų fizinio praradimo;

4.2.3. įvertina patirtą žalą;

4.2.4. imasi veiksmų techninėms priemonėms ir ryšiai atstatyti;

4.2.5. nedelsiant informuojama už serverių ir IT priežiūrą atsakingus asmenys bei reikiamas avarinės tarnybas.

4.3. Bendrovei praradus patalpas Bendrovės vadovas turi organizuoti Įmonės darbą nuotoliniu būdu arba darbą iš laikinų patalpų.

4.4. Bendrovė, per protingą terminą, informuoja Klientus apie Bendrovės patalpų praradimą ir šio praradimo reikšmę Bendrovės klientams.

5. BENDROVĖS DARBUOTOJŲ NEGALĖJIMAS VYKDYTI SAVO FUNKCIJŲ

5.1. Bendrovės vadovas turi imtis priemonių, kad tais atvejais, kai Bendrovės darbuotojai dėl bet kokių priežasčių negali vykdyti savo darbo funkcijų, jų funkcijas galėtų perimti pats Bendrovės vadovas arba kitas Bendrovės darbuotojas.

5.2. Bendrovės darbuotojo negalėjimo vykdyti savo funkcijų atveju, įvertinama patirta žala, jei tokia būtų. Bendrovės vadovas nedelsiant įvertina, ar:

5.2.1. Bendrovės darbuotojų funkcijų nevykdymas gali daryti įtaką Bendrovės veiklos vykdymui ir / ar Ypatingos svarbos paslaugų teikimui;

5.2.2. kokias Bendrovės darbuotojo funkcijas būtų galima perduoti kitam Bendrovės darbuotojui;

5.2.3. ar yra poreikis priimti kitą darbuotoją atlikti reikalingas darbo funkcijas.

5.3. Atlikus 5.2.1 – 5.2.3 p. nurodytus vertinimus, Bendrovės vadovas gali:

5.3.1. perduoti darbuotojo darbo funkcijas kitam darbuotojui (-ams);

5.3.2. priimti kitą darbuotoją ir jam perduoti darbuotojo darbo funkcijas;

5.3.3. perduoda darbuotojo darbo funkcijas išorės paslaugų teikėjui.

5.4. Esant itin skubiam ir neatidėliotinam darbuotojo poreikiui, Bendrovės vadovas ieško alternatyvų (pvz., paslaugos įsigijimo iš trečiųjų asmenų, darbuotojų nuomos) tol, kol bus surastas reikiamas darbuotojas. Kol bus pradėtos teikti paslaugos ar įdarbintas darbuotojas, reikiamos vykdyti funkcijos turi būti proporcingai paskirstomos kitiems (esamiems) Bendrovės darbuotojams.

5.5. Siekiant užtikrinti galimybę Bendrovės vadovui ar kitam darbuotojui perimti darbuotojo funkcijas, dokumentai ir informacija, su kuria darbuotojai dirba, nuolat turi būti prieinami Bendrovės vadovui arba bent vienam kitam darbuotojui (pvz., laikomi Bendrovės serveriuose, debesijos platformose, laikomi fizine ar elektronine forma suteikiant nuolatinę prieigą Bendrovės vadovui arba kitam darbuotojui).

5.6. Apie Bendrovės darbuotojų negalėjimą vykdyti savo funkcijų, Bendrovės klientai yra informuojami tik išimtinais atvejais, kai įvertinus patirtą žalą (jei tokia yra) bei nustačius, kad darbuotojų negalėjimas vykdyti savo funkcijų turi esminės reikšmės Bendrovės veiklos vykdymui ar bei Platformos paslaugų teikimui.

6. TECHNINĖS ĮRANGOS GEDIMAI

6.1. Sutrikus elektros tiekimui Bendrovės patalpose, Bendrovės vadovas, ar jo paskirtas asmuo, nedelsiant informuoja Bendrovės patalpų pastato valdytoją. Jeigu elektros tiekimas neatstatomas per 24 val., Bendrovės vadovas, siekdamas užtikrinti veiklos tęstinumą, gali skelbti darbo vietų evakuaciją.

6.2. Bendrovės vadovas užtikrina, kad sugedus techninei įrangai, kuri reikalingą Bendrovės darbuotojų funkcijų atlikimui, būtų sudaroma galimybė naudotis atsargine techninę įranga arba, kad techninė įranga būtų pataisoma arba pakeičiama per 24 val.

6.3. Informacinių sistemų veiklos tęstinumą užtikrina Bendrovės pasitelktas IT paslaugų tiekėjas. Jeigu dėl ryšio paslaugų sutrikimo nutrūksta interneto ryšys su Bendrovės naudojamais serveriais, Bendrovės vadovas nedelsiant informuoja interneto ryšį Bendrovei tiesiogiai tiekiantį operatorių ir deda visas pastangas interneto ryšio tiekimui atstatyti. Jeigu ryšio paslaugų tiekimas neatstatomas per 24 val., Bendrovės vadovas, siekdamas užtikrinti veiklos tęstinumą, privalo pasitelkti alternatyvų

ryšio paslaugų teikėją (galintį pasiūlyti skubų ir saugų techninį sprendimą šiai situacijai spręsti), o nesant jokioms realioms ryšio paslaugų teikimo alternatyvoms – gali skelbti darbo vietų evakuaciją.

6.4. Jei techninės įrangos gedimai ar sutrikimai turi esminės reikšmės Bendrovės veiklos vykdymui ar Bendrovės Ypatingos svarbos paslaugų teikimui, Bendrovė apie gedimus ar sutrikimus per protingą terminą informuoja savo klientus, nurodant sutrikimų reikšmę Bendrovės teikiamoms paslaugoms.

6.5. Apie Bendrovės darbuotojų negalėjimą vykdyti savo funkcijų, Bendrovės Klientai yra informuojami tik išimtinais atvejais, kai įvertinus patirtą žalą (jei tokia yra) bei nustačius, kad darbuotojų negalėjimas vykdyti savo funkcijų turi esminės reikšmės Bendrovės veiklos vykdymui ar bei Platformos paslaugų teikimui.

7. PLATFORMOS SUTRIKIMAI

7.1. Sutrikus Platformai ar tam tikriems jos funkcionalumams, tai pastebėjęs Bendrovės darbuotojas nedelsiant informuoja Bendrovės vadovą. Bendrovės vadovas imasi atitinkamų priemonių, kad apie Platformos ar jos veiklos sutrikimus nedelsiant, tačiau ne vėliau kaip per 12 val., būtų informuojami Bendrovės Klientai.

7.2. Sutrikus Platformos veiklai, Bendrovės vadovas nedelsiant kreipiasi į Bendrovės IT paslaugų teikėją su prašymu pašalinti Platformos ar atitinkamų jos funkcionalumų sutrikimus.

7.3. Tais atvejais, jei dėl Platformos ar jos funkcionalumų sutrikimų nebuvo įmanoma finansuoti (arba užbaigti pradėto finansavimo) Platformoje skelbiamų projektų, Bendrovės vadovo įsakymu gali būti papildomai (atitinkamai minėtų Platformos ar jos funkcionalumų sutrikimų laikui) pratęstas šių Platformoje skelbiamų projektų finansavimo terminai. Apie tokio sprendimo priėmimą nedelsiant informuojami visi Bendrovės Klientai.

7.4. Apie planuojamus Platformos atnaujinimo, keitimo ar techninės priežiūros darbus, dėl kurių gali sutrikti Platformos veikla Bendrovės vadovas arba jo paskirtas asmuo iš anksto informuoja Klientus, informaciją apie tai paskelbiant Platformoje.

8. DUOMENŲ PRARADIMAS

8.1. Siekiant apsisaugoti nuo duomenų praradimo incidentų pasekmių Bendrovės vadovas Bendrovės veikloje įdiegia technines duomenų saugumo užtikrinimo priemonės, kurios sukuria galimybę:

8.1.1. informaciją, kurią Bendrovė ir jos darbuotojai naudoja savo veikloje, periodiškai, bent vieną kartą per parą, kopijuoti ir ją saugoti išoriniame ir (arba) vidiniame Bendrovės serveryje (duomenų kopijų darymas);

8.1.2. prarastus duomenis ir informaciją atkurti per ne vėliau kaip 24 val.

8.2. Duomenų praradimo atveju informuojami serverio administravimo paslaugas Bendrovei teikiantys subjektai ir/ar IT paslaugas Bendrovei teikiantys subjektai (priklausomai nuo duomenų praradimo pobūdžio) ir nustatomas konkretus duomenų atkūrimo terminas.

8.3. Įvykus incidentui, kai duomenys galimai nuteka ar yra perimami trečiųjų asmenų (kuomet yra galima bet kokia nesankcionuota prieiga prie duomenų), Bendrovės vadovas atlieka šiuos veiksmus:

8.3.1. įvertina ar šio incidento metu nutekėjusių arba perimtų duomenų apimtį;

8.3.2. nustato ar incidento metu kokia nors apimtimi nutekėjo (ar galėjo nutekėti) arba buvo perimti (ar galėjo būti perimti) asmens duomenys. Jeigu taip, dėl galimo asmens duomenų pažeidimo Bendrovės vadovas ir kiti Bendrovės darbuotojai vadovaujasi Bendrajame duomenų apsaugos reglamente bei Bendrovės viduje patvirtintose asmens duomenų pažeidimo valdymo procedūromis;

8.3.3. imasi veiksmų išsiaiškinti, kaip buvo pažeistas duomenų saugumas ir ištaiso saugumo spragą;

8.3.4. blokuoja paskyras, kurių prisijungimo duomenys galėjo būti atskleisti dėl spragos, imasi veiksmų pakeisti šių paskyrų prisijungimo duomenys;

8.3.5. Klientams praneša apie laikinus sistemos sutrikimus, jei dėl keitimo laikinai apribojamos sistemos funkcijos;

8.3.6. įvertina poreikį pateikti teisminius ieškinius trečiosioms šalims, kreiptis į teisėsaugos ir ikiteisminio tyrimo institucijas.

9. MOKĖJIMO PASLAUGŲ BEI TAPATYBĖS NUSTATYMO PASLAUGŲ TEIKĖJO VEIKLOS SUTRIKIMAI

9.1. Bendrovės veikloje egzistuoja rizika, kad išorės subjektai, teikiantys mokėjimo paslaugas, Kliento asmens tapatybės nustatymo paslaugas, gali nutraukti veiklą ar bendradarbiavimą su Bendrove, taip pat gali sutrikti jų paslaugų teikimas. Bendrovė, siekdama išvengti veiklos sutrikimų dėl tokių atvejų, imasi tokių veiksmų:

9.1.1. turi technines galimybes ir pasirengimą dalį paslaugų tiekėjų teikiamų paslaugų perimti ir vykdyti vidiniais resursais (pvz., dalies klientų tapatybę nustatyti fiziškai jiems dalyvaujant ir pan.);

9.1.2. nuolat palaiko ryšį su alternatyviais paslaugų teikėjais ir žino jų galimų teikti paslaugų apimtį. Tuo tarpu, esant galimybei, sudaro sutartis su keliais paslaugų tiekėjais (kurių vienas – pagrindinis, o kiti yra alternatyvūs). Turi būti užtikrinama, kad esant minėtų funkcijų sutrikimams Bendrovė galėtų paslaugų teikimą (visa apimtimi ar bent iš dalies) perkelti pas kitą paslaugos teikėją.

9.2. Sutrikus mokėjimo paslaugų tiekėjo veiklai, Bendrovės vadovas nedelsiant kreipiasi į paslaugų tiekėją ir aiškinasi sutrikimo priežastis ir jų pašalinimo terminus. Nustačius, kad sutrikimas negali būti pašalintas per kelių valandų laikotarpį, Bendrovė surenkamus mokėjimus, esant galimybei, nukreipia pas kitą mokėjimo paslaugų teikėją (į jo sistemoje atidarytą sąskaitą, skirtą sutelktinio finansavimo lėšoms administruoti) ir apie tai nedelsiant informuoja Klientus.

9.3. Mokėjimo paslaugų partneriui užlaikius klientams mokėtinas lėšas ilgiau nei 24 val., esant poreikiui, gali būti inicijuojamas Bendrovės papildomas finansavimas, užtikrinant savalaikį atsiskaitymą su Klientais.

9.4. Sutrikus Kliento tapatybę padedančio nustatyti paslaugų teikėjo veiklai, Bendrovės vadovas pirmiausia kreipiasi į paslaugos tiekėją ir aiškinasi sutrikimo priežastis ir jų pašalinimo terminus. Nustačius, kad sutrikimas negali būti pašalintas per kelių valandų laikotarpį, Bendrovė Kliento tapatybę gali nustatyti pati (pavyzdžiui, fizinis kliento identifikavimas) arba nukreipia Klientus į kito paslaugų tiekėjo, teikiančio tapatybės nustatymo paslaugas, sistemą.

9.5. Jei nėra galimybės surenkamus mokėjimus nukreipti pas kitą mokėjimo paslaugų teikėją, ar Bendrovei ir / ar paslaugų teikėjui nesugebant vykdyti Kliento tapatybės nustatymo, Bendrovės vadovas imasi atitinkamų priemonių, kad apie tai per protingą terminą būtų informuojami Bendrovės Klientai.

10. KIBERNETINĖS ATAKOS IR IT TECHNOLOGIJŲ SUTRIKIMAI

10.1. Bendrovės darbuotojas, pastebėjęs prieš Bendrovę vykdomą ar įvykusią kibernetinę ataką ar aptikęs Bendrovės sistemose bet kokio pobūdžio virusą, nedelsiant apie tai praneša Bendrovės technologijų vadovui.

10.2. Bendrovės technologijų vadovas, gavęs Plano 10.1 p. numatytą pranešimą, nedelsiant, bet ne vėliau kaip per 2 valandas, imasi šių veiksmų:

10.2.1. įvertina kibernetinės atakos ir (ar) viruso galimą poveikį, atsiradimo priežastis bei susisiekia su Bendrovės pasitelktais IT paslaugų teikėjais;

10.2.2. imasi bet kokiu tolesnių veiksmų, būtinų paveiktų Bendrovės funkcijų ir (ar) paslaugų atkūrimui;

10.2.3. informuoja Bendrovės vadovą apie gautą pranešimą.

10.3. Bendrovės technologijų vadovas atlikęs Plano 10.2.1 p. numatytą vertinimą, taip pat sudaro planą priemonių, kurias galima įgyvendinti, kad ateityje būtų išvengta panašaus tipo kibernetinių atakų ar virusų bei pateikia šį planą Bendrovės vadovui, kuris yra atsakingas už jo įgyvendinimą. Jeigu tai yra reikalinga, Bendrovės technologijų vadovas bei Bendrovės vadovas taip pat konsultuojasi su IT paslaugų teikėjais ir specialistais atitinkamų planų ir priemonių sudarymui bei įgyvendinimui.

10.4. Tam, kad būtų išvengta kibernetinių atakų ar virusų Bendrovės vadovas, konsultuodamasis Bendrovės technologijų vadovu ar išorės paslaugų teikėjais, privalo užtikrinti šių prevencinių priemonių įgyvendinimą:

10.4.1. periodinius Bendrovės darbuotojų apmokymus kibernetinio saugumo klausimais. Šie mokymai turėtų būti organizuojami bent kartą per metus. Mokymams Bendrovės vadovas gali pasitelkti kibernetinio saugumo specialistus;

10.4.2. pasirinkti patikimus ir rinkoje žinomus IT paslaugų teikėjus, kurie maksimaliai užtikrintų Bendrovės IT sistemų apsaugą nuo kibernetinių atakų ir (ar) virusų;

10.4.3. pasitelkti IT paslaugų teikėjus periodiniam IT sistemų saugumo audito atlikimui, kurio metu būtų įvertinamas Bendrovės IT sistemų saugumas kibernetinių atakų ir virusų atžvilgiu. IT sistemų saugumo auditas Bendrovėje turėtų būti atliekamas bent kartą per metus.

10.5. Bendrovė savo veikloje taip pat taiko šias prevencines priemones, kurios padeda išvengti kibernetinių atakų:

10.5.1. vykdomi darbuotojų apmokymai, orientuoti į kibernetinių atakų tipus, jų atpažinimo bei pastebėjimo galimybes, prevencinius veiksmus virusų išvengimui ir pan.;

10.5.2. užtikrina, kad Bendrovėje būtų visi esminiai IT sprendimai, apsaugantys Bendrovę nuo kibernetinių atakų ir (ar) virusų, įskaitant, bet neapsiribojant, ugniasienes, antivirusines programas;

10.5.3. pasirenka patikimus IT paslaugų teikėjus bei periodiškai atlieka IT sistemų saugumo analizę.

10.6. Be kita ko, Bendrovė savo veikloje naudodama IT sprendimus visais atvejais vadovaujasi šiais principais ir saugos priemonėmis:

10.6.1. **IP filtravimas.** Į Bendrovės naudojamų IT sistemų administracines (valdymo) zonas galima patekti tik su iš anksto patvirtintais IP adresais. Šiam tikslui nustatomi asmenys ir ryšio taškai, kuriems suteikiama prieiga (pvz., leidžiama prisijungti tik iš anksto nustatytų darboviečių IP adresų, naudojamasi virtualiu privačiu tinklu (angl. *VPN*);

10.6.2. **Ribotos prieigos**. Bendrovėje nėra sukuriamos galimybės prie Bendrovės naudojamų duomenų bazių prisijungti iš išorės. Prisijungti prie Bendrovės naudojamų duomenų bazių gali tik iš anksto patvirtinti asmenys ir iš anksto žinomų lokacijų;

10.6.3. **Šifravimas (SSL sertifikatas).** Bendrovės svetainė, kurioje bus pasiekiamos Bendrovės teikiamos paslaugos, veiks su SSL (angl. *Secure Sockets Layer*) sertifikato pagalba. SSL sertifikatas, be kita ko, padės užšifruoti tarp kliento ir platformos serverio siunčiamą informaciją. Naršymas ir kiti Bendrovės svetainėje atliekami veiksmai šifruojami naudojantis SSL sertifikatu;

10.6.4. **Stebėsena.** Bendrovės svetainėje įdiegiama sistema, kuria naudojantis galima stebėti vartotojų prisijungimus (prisijungimo / atsijungimo laikas ir data), matyti vartotojų atliekamus veiksmus (redaguojamus elementus, patvirtinimus, nurodymus, mokėjimus);

10.6.5. **Slaptažodžiai.** Siekiant apsisaugoti nuo sukčiavimo ir kitų operacinių rizikų, iš Bendrovės klientų bus reikalaujama padidinto slaptažodžių sudėtingumo, t. y. slaptažodžiai turi būti kompleksiški, sudaryti iš 8 ir daugiau simbolių, įskaitant didžiąsias ir mažąsias raides, skaitmenis ir papildomus specifinius simbolius. Taip pat papildomai naudojama antrinio slaptažodžio (angl. *two-factor authentication*) technologija.

10.6.6. **Prisijungimo apsauga.** Bendrovės darbuotojų ir sistemų atžvilgiu prisijungiant prie išorinio tinklo visais atvejais naudojamos ugniasienės (angl. *firewall*).

11. POVEIKIO BENDROVĖS VEIKLAI ANALIZĖ

11.1. Siekiant užtikrinti tinkamą Bendrovės veiklos tęstinumo valdymą, Bendrovės vadovas taip pat periodiškai atlieka galimų incidentų poveikio Bendrovės veiklai analizę, kurios metu įvertina Bendrovės veiklos sutrikimų galimą poveikį konfidencialumui, vientisumui ir prieinamumui.

11.2. Poveikio veiklai analizė yra atliekama remiantis tiek vidaus, tiek išorės duomenimis, kuriuos gali pateikti trečiosios šalys. Poveikio veiklai analizės metu Bendrovės vadovas taip pat įvertina nustatytų ir klasifikuotų veiklos funkcijų, pagalbinių procesų, trečiųjų šalių ir informacinių išteklių svarbą ir jų tarpusavio priklausomybės ryšius.

11.3. Bendrovės vadovas taip pat užtikrina, kad atsižvelgiant į poveikio veiklai analizę, Bendrovėje būtų įdiegtos tinkamos informacinių ir ryšių technologijų sistemos, užtikrinančios tinkamą Bendrovės veiklos ir/ar atskirų funkcijų sutrikimų prevenciją.

11.4. Bendrovės vadovas, atsižvelgdamas į poveikio veiklai analizę, taip pat sprendžia dėl poreikio koreguoti šį Planą, numatant papildomas priemones, skirtas minimizuoti riziką Bendrovei patirti bet kokio pobūdžio neigiamą poveikį dėl Bendrovės veiklos ir/ar atskirų funkcijų sutrikimo. Esant

poreikiui, Bendrovės vadovas naujai apibrėžia veiklos funkcijas, pagalbinius procesus ir/ar kitas aktualias veiklos tęstinumui užtikrinti procedūras.

12. BAIGIAMOSIOS NUOSTATOS

12.1. Šis Planas tvirtinamas ir/ar keičiamas Bendrovės vadovo įsakymu. Plano pakeitimai įsigalioja Bendrovės įsakymo dieną, jeigu atitinkamame įsakyme nėra nurodyta kitaip.

12.2. Planas turi būti atnaujintas atsižvelgiant į patirtį, įgytą valdant incidentus, nustatytas nauja rizika ir/ar grėsmes bei organizacinius pokyčius.

12.3. Šis Planas yra skelbiamas Platformoje.

12.4. Su šia Politika pasirašytinai privalo būti supažindinti visi Bendrovės darbuotojai bei akcininkai.

12.5. Bendrovės vadovas yra atsakingas už periodinį Plano testavimą ir atnaujinimą. Plano testavimas atliekamas ne rečiau kaip kartą per metus.

12.6. Bendrovės vadovas sudaro sąrašą kontaktinių asmenų, su kuriais būtina nedelsiant palaikyti ryšį įvykus konkrečiam Bendrovės veiklos sutrikimui. Pasikeitus šių kontaktinių asmenų duomenims / paslaugos teikėjams, Bendrovės vadovas nedelsiant atnaujina atitinkamą kontaktinių asmenų sąrašą.

12.7. Su šiuo Planu pasirašytinai privalo būti supažindinti visi Bendrovės darbuotojai bei akcininkai.

12.8. Bendrovės vadovas yra atsakingas už periodinį Plano testavimą ir atnaujinimą. Plano testavimas atliekamas ne rečiau kaip kartą per metus.