

VEIKLOS TĘSTINUMO PLANAS

1. BENDROSIOS NUOSTATOS

- 1.1. Šis UAB Crowdpear („**Bendrovė**“) veiklos tęstinumo planas („**Planas**“) nustato:
 - 1.1.1. Bendrovės darbuotojų veiksmus, pareigas ir atsakomybes užtikrinant ir įgyvendinant Bendrovės veiklos tęstinumą ekstremalių situacijų atvejais;
 - 1.1.2. informavimo ir veiklos sutrikimo šalinimo veiksmus ekstremalių situacijų atvejais, siekiant užtikrinti nepertraukiamą Bendrovės veiklą ir apriboti nuostolius veiklos sutrikimų atveju.
- 1.2. Remiantis Bendrovės atlikta poveikio veiklai analize, Bendrovė šiuo Planu siekia užtikrinti, kad Bendrovės, kaip sutelktinio finansavimo platformos operatoriaus, funkcijos būtų atliekamos nenutrūkstamai bei Bendrovėje būtų aiškiai identifiкуotos rizikos, galinčios padaryti neigiamą poveikį Bendrovės veiklai, taip pat Bendrovės informacinių ir ryšių technologijų sistemoms.
- 1.3. Bendrovės vadovas atsako už šio Plano įgyvendinimą.
- 1.4. Tuo atveju, jeigu Bendrovės vadovas dėl objektyvių priežasčių negali atlikti savo funkcijų (atostogauja, serga ir pan.), Bendrovės vadovas iš anksto paskiria Bendrovės darbuotoją, atsakingą už visų šiame Plane numatytų funkcijų įgyvendinimą.

2. SAŲOKOS

- 2.1. Jei kontekstas nereikalauja kitaip, šiame Plane didžiosiomis raidėmis vartojamos sąvokos turi žemiau nurodytas reikšmes:
 - 2.1.1. **Bendrovė (Operatorius)** – sutelktinio finansavimo platformo UAB Crowdpear operatorius, sutelktinio finansavimo paslaugų teikėjas UAB Crowdpear, juridinio asmens kodas 305888586, buveinė registruota adresu Kareivių g. 11B, Vilnius, Lietuva;
 - 2.1.2. **Finansuotojas (Investuotojas)** – Naudotojas (Bendrovės klientas), Sutelktinio finansavimo lėšomis finansuojantis Platformoje paskelbtą Projektą;
 - 2.1.3. **Reglamentas** – Europos Parlamento ir Tarybos Reglamentas (ES) 2020/1503 dėl Europos sutelktinio finansavimo paslaugų verslui teikėjų, kuriuo iš dalies keičiamas Reglamentas (ES) 2017/1129 ir Direktyva (ES) 2019/1937;
 - 2.1.4. **Planas** – UAB Crowdpear veiklos tęstinumo planas;
 - 2.1.5. **Platforma** – Operatoriaus administruojama sutelktinio finansavimo platforma, prieinama adresu <https://crowdpear.com/>, per kurią Finansuotojai gali suteikti Sutelktinio finansavimo lėšų Projekto savininkui, finansuodami jo Projektą;
 - 2.1.6. **Projektas** – verslo reikmėms, išskyrus vartojimą, tenkinti parengtas ir Platformoje paskelbtas Projektas, kuriam įgyvendinti Projekto savininkas iš Finansuotojų siekia pritraukti Sutelktinio finansavimo lėšas;
 - 2.1.7. **Projekto savininkas** – Naudotojas (Bendrovės klientas), kuris inicijuoja ir per Platformą paskelbia Projektą, siekdamas iš Finansuotojų pritraukti Sutelktinio finansavimo lėšų;
 - 2.1.8. **Operacinė rizika** – nuostolių, verslo procesų sutrikimo, neigiamo poveikio reputacijai rizika / tikimybė dėl žmonių, sistemų, netinkamų ar nepavykusių vidaus procesų arba dėl išorės įvykių įtakos, įskaitant teisinę riziką.
- 2.2. Kitos šiame Plane vartojamos sąvokos suprantamos taip, kaip jos apibrėžtos Reglamente ar kituose taikytinuose teisės aktuose.

3. RIZIKŲ ANALIZĖ

- 3.1. Bendrovės veiklos tęstinumo planavimas grindžiamas galimo poveikio Bendrovės veiklai vertinimu ir analize. Bendrovės veiklos sutrikimai visais atvejais yra vertinami atsižvelgiant į:
 - 3.1.1. finansinį poveikį;
 - 3.1.2. poveikį Bendrovės vykdomai veiklai ir (ar) teikiamoms paslaugoms;
 - 3.1.3. kaštus, kurie gali būti reikalingi Bendrovės veiklos 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. Siekiant užtikrinti Bendrovės veiklos tęstinumą, Bendrovės vadovas periodiškai, tačiau ne rečiau kaip kartą per metus analizuoja aplinkybes ir situacijas, susijusias su Bendrovės operacinės rizikos atsiradimu, jų tikimybe.
- 3.3. 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.

4. POVEIKIO VEIKLAI ANALIZĖ

- 4.1. Siekdamas užtikrinti patikimą 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.
- 4.2. Poveikio veiklai analizė yra atliekama remiantis tiek vidaus, tiek išorės duomenimis, kuriuos gali pateikti trečiosios šalys (pvz., Bendrovės pasitelkiami išorės paslaugų teikėjai).
- 4.3. 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.
- 4.4. 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.
- 4.5. Bendrovės vadovas, atsižvelgdamas į poveikio veiklai analizę, taip pat sprendžia dėl poreikio koreguoti šį Planą, numatant papildomas priemones, skirtas minimizuoti riziką Bendrovei patirti neigiamą poveikį dėl Bendrovės veiklos ir (ar) atskirų funkcijų sutrikimo. Esant poreikiui, Bendrovės vadovas naujai apibrėžia veiklos funkcijas, pagalbinius procesus ir kitus veiklos tęstinumui užtikrinti svarbius procesus.

5. PAGRINDINĖS FUNKCIJOS, KURIOMS BŪTINAS OPERATYVUS NEPERTRAUKIAMAS VEIKLOS TĘSTINUMO UŽTIKRINIMAS

- 5.1. Pagrindinės funkcijos, kurioms būtinas operatyvus nepertraukiamas veiklos tęstinumo užtikrinimas, yra šios:

Funkcija	Galimas poveikis Bendrovės veiklai
Galimybė Bendrovės klientams (Finansuotojams ir Projektų savininkams) prisijungti prie savo paskyros Platformoje	Vidutinis
Pagrindinės informacijos (turimos paskolos, lėšų likučiai, suteiktų paskolų portfelis) atvaizdavimas Bendrovės klientų (Finansuotojų ir Projektų savininkų) Platformos paskyroje	Žemas

Galimybė Bendrovės klientams Platformoje vykdyti pagrindines operacijas – finansuoti ir gauti finansavimą Projektams	Aukštas
Nepertraukiamas informacijos apie Bendrovės klientus ir jų atliktas operacijas registravimas ir saugojimas	Vidutinis
Bendrovės ūkinės veiklos operacijų valdymas	Vidutinis
Bendrovės klientų (Finansuotojų ir Projektų savininkų) identifikavimas bei tapatybės nustatymas	Aukštas

5.2. Poveikio veiklai analizės metu Bendrovė identifikavo žemiau nurodytus verslo procesus, turinčius esminę įtaką Bendrovės veiklai:

	Verslo procesas	Aprašymas
	Klientų registracija / aptarnavimas	
1.	Kliento registracija	Nenutrūkstama Bendrovės kliento (Finansuotojo ar Projekto savininko) registracija bei duomenų saugojimas
2.	Kliento identifikacija (KYC procesas)	Nenutrūkstama kliento identifikacijos (KYC) procedūra, apimanti reikalingos informacijos bei duomenų surinkimą ir identifikavimo priemonių naudojimą pagal Bendrovės pinigų plovimo prevencijos procedūras
3.	Kliento prisijungimas	Galimybė Bendrovės klientams (Finansuotojams bei Projektų savininkams) prisijungti prie savo paskyrų Platformoje
	Projektų skelbimas ir finansavimas	
4.	Projekto sukūrimas	Galimybė Projektų savininkams pateikti informaciją apie savo Projektus ir skelbti ją Bendrovės Platformoje po Bendrovės įvertinimo
5.	Informacijos apie Projektus atnaujinimas	Galimybė Projektų savininkams atnaujinti informaciją apie savo Projektus, paskelbtą Bendrovės Platformoje
6.	Lėšų įnešimas	Galimybė Finansuotojams įnešti lėšas į savo mokėjimo sąskaitas (valdomas išorės mokėjimo paslaugų teikėjo) siekiant šias lėšas investuoti į Platformoje skelbiamus projektus, taip pat galimybė Projektų savininkams įnešti lėšas į savo mokėjimo sąskaitas (valdomas išorės mokėjimo paslaugų teikėjo) siekiant naudoti šias lėšas mokesčių, kuriuos taiko Bendrovė, apmokėjimui
7.	Lėšų išėmimas	Galimybė Finansuotojams išsiimti lėšas iš savo mokėjimo sąskaitų (valdomų išorės mokėjimo paslaugų teikėjo), skirtas Bendrovės Platformoje skelbiamų Projektų finansavimui, taip pat galimybė Projektų savininkams išsiimti lėšas iš savo mokėjimo sąskaitų (valdomų išorės mokėjimo paslaugų teikėjų),

		kurios gautos kaip paskola po sėkmingo Projekto sufinansavimo Platformoje ar kurios buvo įneštos paties Projekto savininko (pvz., su tikslu sumokėti taikomus mokesčius)
8.	Projekto finansavimas	Galimybė Finansuotojams investuoti į Bendrovės Platformoje skelbiamus Projektus
9.	Lėšų pervedimas Projekto savininkui	Galimybė pervesti Projekto savininkui lėšas, surinktas sėkmingai finansavus Projektą
10.	Palūkanų mokėjimas Finansuotojams	Galimybė Projektų savininkams mokėti palūkanas (taip pat bet kokius kitus mokesčius, mokėtinus Finansuotojams ar Bendrovei) pagal Platformoje sudarytas paskolos sutartis
Klientų paskyrų palaikymas		
11.	Paskyros slaptažodžio keitimo procesas	Galimybė klientams pasikeisti slaptažodžius, naudojamus prisijungiant prie Platformoje registruotų paskyrų
12.	Kontaktinės informacijos atnaujinimas	Galimybė klientams atnaujinti savo kontaktinę informaciją, pateiktą registruojantis Platformoje
13.	Informacijos apie Projektus pateikimas	Galimybė pateikti Bendrovės klientams informaciją (jų Platformoje registruotose paskyrose) apie projektus, į kuriuos klientai yra investavę arba kurių savininkais patys yra
Duomenų saugojimas		
14.	Duomenų saugojimas	Galimybė Bendrovei saugiai saugoti informaciją apie Bendrovės klientus, jų atliktas operacijas, finansuotus projektus ir bet kokią kitą informaciją, susijusią su Bendrovės veikla
Klientų aptarnavimas		
15.	Klientų skundų nagrinėjimas	Galimybė gauti klientų skundus ir tinkamai juos išnagrinėti
Pardavimų procesas		
16.	Pasiūlymų teikimas	Galimybė pateikti finansavimo sąlygas potencialiems Bendrovės klientams (Projektų savininkams)
17.	Derybų procesas	Galimybė tinkamai vesti derybas su potencialiais Bendrovės klientais (Projektų savininkais)
Apskaita		
18.	Apskaitos procesas	Galimybė tinkamai vesti apskaitos procedūras Bendrovės veikloje
19.	Sąskaitų išrašymo procesas	Galimybė tinkamai išrašyti sąskaitas Bendrovės klientams ir susijusioms šalims

6. NENUTRŪKSTAMOS VEIKLOS UŽTIKRINIMO PRIEMONĖS

- 6.1. Bendrovė, siekdama užtikrinti nenutrūkstamą savo, kaip sutelktinio finansavimo platformos operatoriaus veiklą, atsižvelgia į operacines rizikas, su kuriomis gali susidurti veiklos metu.
- 6.2. Bendrovė identifikuoja šias operacines rizikas kaip vienas pagrindinių rizikų:
 - 6.2.1. Bendrovės darbuotojų negalėjimas vykdyti savo funkcijų;
 - 6.2.2. Bendrovės patalpų praradimas;
 - 6.2.3. techninės įrangos gedimai;
 - 6.2.4. kibernetinės atakos;
 - 6.2.5. Platformos funkcionalumo sutrikimai;
 - 6.2.6. duomenų praradimas;
 - 6.2.7. mokėjimo ir tapatybės nustatymo paslaugų teikėjų veiklos sutrikimai.
- 6.3. Bendrovė supranta, jog šio Plano 6.2 p. nurodytas rizikų sąrašas nėra baigtinis. Jeigu materializuotųsi kitos (šiam Plane tiesiogiai neįvardytos) Bendrovės operacinės rizikos, Bendrovės darbuotojai privalo tinkamai reaguoti pagal analogiją laikydamiesi šiame Plane numatytų bendrųjų principų ir procedūrų.
- 6.4. Jeigu Bendrovė susiduria su mokumo problemomis arba Bendrovei iškyla bankroto rizika, kuo operatyviau ieškomas kitas subjektas, galintis vykdyti sutelktinio finansavimo platformos operatoriaus funkcijas Reglamente ir kituose teisės aktuose numatyta tvarka. Platformos administravimo perdavimas kitam subjektui, turinčiam teisę administruoti sutelktinio finansavimo platformą, jokia būdu negali pabloginti Bendrovės klientų (Finansuotojų ir Projektų savininkų) padėties.

7. BENDROVĖS DARBUOTOJŲ NEGALĖJIMAS VYKDYTI SAVO FUNKCIJŲ

- 7.1. Bendrovės vadovas privalo užtikrinti, kad tais atvejais kai Bendrovės darbuotojai dėl bet kokių priežasčių negalės vykdyti savo funkcijų, jų funkcijas nedelsiant galėtų perimti kitas Bendrovės darbuotojas arba pats Bendrovės vadovas, kol bus atkurtas reikiamas personalo kiekis Bendrovės veikloje esančių funkcijų vykdymui.
- 7.2. Bendrovės darbuotojo negalėjimo vykdyti savo funkcijų atveju, įvertinama patirta žala, jei tokia būtų.
- 7.3. Bendrovės vadovas Bendrovės darbuotojo negalėjimo vykdyti savo funkcijų atveju nedelsiant, bet ne vėliau kaip per 1 (vieną) darbo dieną, taip pat įvertina, ar:
 - 7.3.1. Bendrovės darbuotojų funkcijų nevykdymas gali daryti įtaką Bendrovės veiklos vykdymui, t. y.:
 - 7.3.1.1. sutelktinio finansavimo sandorių sudarymui Bendrovės administruojamoje Platformoje;
 - 7.3.1.2. Projektų savininkų patikimumo vertinimo procesui;
 - 7.3.1.3. pinigų plovimo ir teroristų finansavimo prevencijos reikalavimų ir susijusių procedūrų įgyvendinimui;
 - 7.3.1.4. Platformoje sudarytų sutelktinio finansavimo sandorių administravimui;
 - 7.3.1.5. komunikacijos su Bendrovės klientais (Finansuotojais, Projektų savininkais) vykdymui;
 - 7.3.1.6. kitoms funkcijoms, kurios yra įgyvendinamos Bendrovei vykdant savo veiklą ir teikiant sutelktinio finansavimo paslaugas.
 - 7.3.2. kokias Bendrovės darbuotojo funkcijas būtų galima perduoti kitam Bendrovės darbuotojui;
 - 7.3.3. ar yra poreikis papildomai priimti kitą darbuotoją, kuris atliktų reikalingas darbo funkcijas.

- 7.4. Esant itin skubiam ir neatidėliotinam personalo poreikiui, Bendrovės vadovas ieško alternatyvų (pavyzdžiui, paslaugos įsigijimo iš trečiųjų asmenų, darbuotojų nuomos) tol, kol bus surastas reikiamas personalo narys. Atitinkamos alternatyvos turi būti įgyvendintos ne vėliau kaip per 2 (dvi) savaites. Kol bus pradėtos teikti paslaugos ar įdarbintas darbuotojas, reikiamos vykdyti funkcijos turi būti nedelsiant, tačiau ne vėliau kaip per 1 darbo dieną, proporcingai paskirstomos kitiems (esamiems) Bendrovės darbuotojams.
- 7.5. Atlikęs 7.3 punkte numatytą vertinimą (ir, esant poreikiui, priėmus kitą darbuotoją), Bendrovės vadovas perduoda Bendrovės darbuotojo, negalinčio vykdyti savo funkcijų, funkcijas kitam darbuotojui (darbuotojams) ir (ar) išoriniam paslaugos teikėjui.
- 7.6. Kol Bendrovėje yra visiškai atkuriamą situacija, susijusi su Bendrovės darbuotojo (-ų) negalėjimu vykdyti savo funkcijų, Bendrovės vadovas turi nuolat stebėti, ar priemonės, kurių ėmėsi atitinkamų funkcijų vykdymo užtikrinimui, leidžia Bendrovei vykdyti savo veiklą bent tokia apimtimi, kuri užtikrintų tinkamą sutelktinio finansavimo paslaugų teikimą.
- 7.7. Prevenciškai Bendrovės vadovas turi reguliariai (ne rečiau kaip 1 (vieną) kartą per mėnesį įvertinti, ar Bendrovėje yra galimybė paskirstyti kiekvieno darbuotojo funkcijas kitiems Bendrovės darbuotojams tuo atveju, jeigu kažkuris Bendrovės darbuotojas negalėtų dėl tam tikrų priežasčių vykdyti savo funkcijų, ir ar toks funkcijų paskirstymas kitiems Bendrovės darbuotojams užtikrintų tinkamą sutelktinio finansavimo paslaugų teikimą ir susijusių procesų užtikrinimą iki kol būtų atkurta pradinė padėtis.
- 7.8. Siekiant užtikrinti galimybę Bendrovės vadovui ar kitam darbuotojui perimti darbuotojo funkcijas, dokumentai ir informacija, su kuria darbuotojai dirba, turi būti prieinami Bendrovės arba bent vienam kitam darbuotojui (pavyzdžiui, laikomi debesijos serveryje, laikomi fizine ar elektronine forma suteikiant nuolatinę prieigą Bendrovės vadovui arba kitam darbuotojui).
- 7.9. Rizikos atžvilgiu Bendrovė vertina, kad Bendrovės darbuotojų negalėjimas vykdyti savo funkcijų yra vidutinio tikėtumo (ilgesniam nei 1 darbo dienos laikotarpiui – mažo tikėtumo), o galimi neigiami padariniai yra žemo lygio.

8. BENDROVĖS VEIKLOS ATSTATYMAS PATALPŲ PRARADIMO ATVEJU

- 8.1. Patalpų praradimo atveju (gaisro, stichinės nelaimės, teroro akto, nusikalstamų veikų ar kitų veiksmų atveju), visų pirma, vykdoma žmonių evakuacija.
- 8.2. Bendrovės vadovas ar jo įgaliotas asmuo priima sprendimą dėl tolimesnių veiksmų, reikalingų veiklos procesams tęsti, išvengti Bendrovės dokumentų praradimo, įvertina patirtą žalą, atstato technines priemones ir ryšius, nedelsiant informuoja už serverių ir IT priežiūrą atsakingus asmenis bei reikiamas avarines tarnybas.
- 8.3. Bendrovei praradus patalpas, Bendrovės vadovas kuo skubiau privalo organizuoti Bendrovės darbą nuotoliniu būdu arba darbą iš laikinų patalpų. Šių alternatyvių darbo sąlygų sukūrimas privalo būti įgyvendintas ne vėliau kaip per 1 darbo dieną. Bendrovės vadovas taip pat privalo užtikrinti, kad pasirinktas darbo organizavimo būdas (nuotolinis darbas, darbas iš laikinų patalpų ar kt.) leistų darbuotojams įgyvendinti jų funkcijas visa apimtimi ir kad atitinkamas darbo organizavimo būdas neribotų Bendrovės veikloje svarbių funkcijų užtikrinimo.
- 8.4. Bendrovės vadovas privalo užtikrinti, kad Bendrovės veikloje naudojami dokumentai, kurie yra esminiai Bendrovės veiklai ar paslaugų teikimui, būtų reguliariai skenuojami ir saugomi elektroniniu būdu Bendrovės serveriuose.
- 8.5. Bendrovės kasdieniui veiklai naudojami dokumentai turi būti saugomi rakinauose spintose. Esant poreikiui, Bendrovės veiklos dokumentai gali būti perduodami trečiajam asmeniui, su kuriuo Bendrovė turi sudariusi dokumentų archyvavimo sutartį.
- 8.6. Maksimalus atkūrimo laikas patalpų praradimo atveju turi būti 24 val.
- 8.7. Tam, kad būtų užtikrintas Bendrovės veiklos atstatymas patalpų praradimo atveju, Bendrovės vadovas privalo imtis prevencinių priemonių, t. y. užtikrinti, kad bent 2/3 Bendrovės darbuotojų turėtų

nešiojamus kompiuterius bei prieigą prie interneto, kuri užtikrintų galimybę Bendrovės darbuotojams vykdyti savo funkcijas nuotoliniu būdu.

- 8.8. Rizikos atžvilgiu Bendrovė vertina, kad patalpų praradimas yra mažo tikėtumo, o galimi neigiami padariniai yra vidutinio lygio.

9. TECHNINĖS ĮRANGOS GEDIMAI AR SUTRIKIMAI

Elektros tiekimo sutrikimas

- 9.1. Sutrikus elektros tiekimui, pirmasis tą pastebėjęs Bendrovės darbuotojas privalo nedelsiant informuoti Bendrovės vadovą.
- 9.2. Bendrovės vadovas nedelsiant informuoja Bendrovės patalpų savininką bei pastato administratorių apie elektros tiekimo sutrikimą. Bendrovės vadovas taip pat komunikuoja su patalpų savininkų ir (ar) pastato administratoriumi dėl tikėtino elektros tiekimo atkūrimo laiko bei apie tai informuoja Bendrovės darbuotojus.
- 9.3. Jeigu elektros tiekimas neatstatomas per 4 val., Bendrovės vadovas gali skelbti darbo vietų evakuaciją bei organizuoti darbą kaip tai numatyta šio Plano 8.3 punkte (pvz., nuotoliniu būdu).
- 9.4. Prevenciškai Bendrovės vadovas užtikrina, kad bent 2/3 Bendrovės darbuotojų turėtų nešiojamus kompiuterius, kurie suteiktų jiems galimybę dirbti ne Bendrovės patalpose sutrikus elektros tiekimui.
- 9.5. Rizikos atžvilgiu Bendrovė vertina, kad elektros tiekimo sutrikimas yra mažo tikėtumo, o galimi neigiami padariniai taip pat yra žemo lygio.

Techninės įrangos sutrikimai

- 9.6. Bendrovės vadovas užtikrina, kad sugedus techninei įrangai, kuri reikalinga Bendrovės darbuotojų funkcijų atlikimui, būtų sudaroma galimybė naudotis atsargine technine įranga arba kad techninė įranga būtų pataisyta arba pakeista per 24 val.
- 9.7. Atitinkamai, Bendrovės vadovas privalo užtikrinti, kad bent 1/3 darbuotojų būtų užtikrinta atsarginė techninė įranga (pvz., nešiojamieji kompiuteriai, mobilieji telefonai ar kita darbuotojo funkcijoms reikalinga įranga).
- 9.8. Rizikos atžvilgiu Bendrovė vertina, kad techninės įrangos sutrikimas yra vidutinio tikėtumo, o galimi neigiami padariniai yra žemo lygio.

Interneto ryšio tiekimo sutrikimai

- 9.9. Informacinių sistemų veiklos tęstinumą užtikrina Bendrovės pasitelktas IT paslaugų teikėjas. 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.
- 9.10. Jeigu ryšio paslaugų tiekimas neatstatomas per 4 val., Bendrovės vadovas privalo pasitelkti alternatyvų ryšio paslaugų teikėją (galintį pasiūlyti skubų ir saugų techninį sprendimą), o nesant jokioms realioms ryšio paslaugų teikimo alternatyvoms – gali skelbti darbo vietų evakuaciją ir organizuoti darbą kaip tai numatyta Plano 8.3 punkte.

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 vadovui ir / ar atsakingam asmeniui.
- 10.2. Bendrovės vadovas / atsakingas asmuo 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 susisieikia su Bendrovės pasitelktais IT paslaugų teikėjais;

- 10.2.2. imasi bet kokių tolesnių veiksmų, būtinų paveiktų Bendrovės funkcijų ir (ar) paslaugų atkūrimui;
 - 10.2.3. informuoja Bendrovės vadovą apie gautą pranešimą, jeigu praešimą gavo atsakingas asmuo.
- 10.3. Bendrovės vadovas / atsakingas asmuo 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. Bendrovės vadovas yra atsakingas už jo įgyvendinimą. Jeigu tai yra reikalinga, 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 su 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 darbuotojų IP adresų, naudojamosi virtualiu privačiu tinklu (angl. *VPN*));
 - 10.6.2. **Ribotos prieigos.** Bendrovėje nėra sukuriama galimybė 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*).
- 10.7. Rizikos atžvilgiu Bendrovė vertina kibernetinių atakų ir IT technologijų sutrikimų tikėtinumą kaip žemą, o galimų neigiamų padarinių – kaip vidutinio lygio.

11. PLATFORMOS FUNKCIONALUMŲ SUTRIKIMAI

- 11.1. Sutrikus Bendrovės valdomos Platformos veikimui, tai pastebėjęs Bendrovės darbuotojas nedelsiant praneša apie tai Bendrovės vadovui, kuris imasi atitinkamų priemonių, kad apie Platformos ar jos veiklos sutrikimus nedelsiant, tačiau ne vėliau kaip per 12 val., būtų informuojami Bendrovės klientai.
- 11.2. Sutrikus Platformos veiklai, Bendrovės vadovas nedelsiant, tačiau ne vėliau kaip per 2 valandas, kreipiasi į Bendrovės IT paslaugų teikėją su prašymu pašalinti Platformos ar atitinkamų jos funkcionalumų sutrikimus.
- 11.3. Jeigu dėl Platformos ar jos funkcionalumų sutrikimų nebuvo įmanoma finansuoti Platformoje skelbiamų Projektų, Bendrovės vadovo įsakymu gali būti papildomai (atitinkamam minėtų Platformos ar jos funkcionalumų sutrikimų laikui) pratęstas atitinkamų Platformoje skelbiamų Projektų finansavimo terminas. Apie tokio sprendimo priėmimą nedelsiant informuojami visi Bendrovės klientai.
- 11.4. Apie planuojamus Platformos atnaujinimo, keitimo ar techninės priežiūros darbus, dėl kurių gali sutrikti Platformos veikla Bendrovės vadovas arba jo paskirtas asmuo iš anksto informuoja Bendrovės klientus, paskelbdamas atitinkamą informaciją Platformoje.
- 11.5. Rizikos atžvilgiu Bendrovė, atsižvelgdama į tai, kad Platformos sukūrimo ir administravimo paslaugą gauna iš patikimo paslaugų teikėjo, tikėtinumo lygį vertina kaip žemą, tačiau galimų neigiamų padarinių rizika Platformos sutrikimų atveju yra aukšta.

12. DUOMENŲ PRARADIMAS

- 12.1. Siekiant apsisaugoti nuo duomenų praradimo incidentų pasekmių, Bendrovės vadovas Bendrovės veikloje įdiegia technines duomenų saugumo užtikrinimo priemones, kurios suteikia galimybę:
- 12.1.1. periodiškai (bent vieną kartą per parą) kopijuoti ir saugoti išoriniame ir (ar) vidiniame Bendrovės serveryje informaciją, kurią Bendrovė ir jos darbuotojai naudoja savo veikloje;
- 12.1.2. prarastus duomenis ir informaciją atkurti ne vėliau kaip per 24 valandas.
- 12.2. 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, kuris negali būti ilgesnis kaip 24 valandos.
- 12.3. Įvykus incidentui, kai duomenys galimai nuteka ar yra perimami trečiųjų asmenų (kuomet yra galima bet kokia Bendrovės nesankcionuota prieiga prie duomenų), Bendrovės vadovas ne vėliau kaip per 24 valandas privalo atlikti šiuos veiksmus:
- 12.3.1. įvertinti atitinkamo incidento metu nutekėjusių arba perimtų duomenų tipą bei apimtį;
- 12.3.2. nustatyti, 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 patvirtintose asmens duomenų pažeidimo valdymo taisyklėse numatytais procedūromis (be kita ko, esant asmens duomenų apsaugos pažeidimui nedelsiant apie tai informuojama Valstybinė duomenų apsaugos inspekcija);

- 12.3.3. imtis veiksmų išsiaiškinti, kaip buvo pažeistas duomenų saugumas ir ištaisyti saugumo spragą;
 - 12.3.4. blokuoti paskyras, kurių prisijungimo duomenys galėjo būti atskleisti dėl spragos, imtis veiksmų pakeisti šių paskyrų prisijungimo duomenis;
 - 12.3.5. Bendrovės klientams nedelsiant pranešti apie laikinus Platformos sutrikimus, jei dėl keitimo laikinai apribojamos Platformos funkcijos;
 - 12.3.6. įvertinti poreikį pateikti teisinius ieškinius trečiosioms šalims, kreiptis į teisėsaugos ir ikiteisminio tyrimo institucijas.
- 12.4. Rizikos atžvilgiu Bendrovė duomenų praradimo tikėtinumą vertina kaip žemą, o jo galimus sukelti neigiamus padarinius kaip vidutinio lygio.

13. PASLAUGŲ TEIKĖJŲ VEIKLOS SUTRIKIMAI

- 13.1. Bendrovė, siekdama išvengti pasitelktų paslaugų teikėjų veiklos sutrikimų (pavyzdžiui, paslaugų teikėjų teikiančių mokėjimo ir (ar) klientų tapatybės nustatymo paslaugas) ar atitinkamų subjektų bendradarbiavimo su Bendrove nutraukimo, imasi tokių prevencinių veiksmų:
- 13.1.1. nuolat palaiko ryšį su alternatyviais paslaugų teikėjais ir žino jų galimų teikti paslaugų apimtį. Esant galimybei, Bendrovė sudaro sutartis su keliais paslaugų teikėjais;
 - 13.1.2. nuolat prižiūri, ar paslaugų teikėjai tinkamai įgyvendina su jais sudarytose sutartyse nustatytus paslaugų teikimo lygius;
 - 13.1.3. užtikrina, kad su paslaugų teikėjų sudarytose sutartyse būtų įtvirtintos nuostatos, susijusios su sutrikimų atkūrimo terminais, pranešimų apie sutrikimus pateikimu ir kt.
 - 13.1.4. užtikrina nuolatinę paslaugų teikėjų teikiamų paslaugų stebėseną;
 - 13.1.5. užtikrina, kad esant minėtų funkcijų sutrikimams Bendrovė galėtų paslaugų teikimą (visa apimtimi ar bent iš dalies) perkelti pas kitą paslaugos teikėją.
- 13.2. Sutrikus mokėjimo paslaugų teikėjo veiklai, Bendrovės vadovas nedelsiant, bet ne vėliau kaip per 2 valandas, kreipiasi į paslaugų teikėją ir aiškinasi sutrikimo priežastis ir jų pašalinimo terminus. Nustačius, kad sutrikimas negali būti pašalintas per kelis 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, ne vėliau kaip per 4 valandas informuoja Bendrovės klientus.
- 13.3. Mokėjimų partneriui užlaikius Bendrovės klientams mokėtinas lėšas ilgiau nei 24 val., esant poreikiui, gali būti inicijuojamas Bendrovės papildomas finansavimas, užtikrinant savalaikį atsiskaitymą su klientais. Toks finansavimas turi būti atliekamas ne vėliau nei per 24 val.
- 13.4. Sutrikus kliento tapatybę padedančio nustatyti paslaugų teikėjo veiklai, Bendrovės vadovas pirmiausia imasi priemonių, kad būtų sustabdyta naujų klientų registracija Platformoje ir neidentifikuoti klientai negalėtų per Platformą teikti finansavimo. Bendrovės vadovas taip pat nedelsiant, bet ne vėliau kaip per 2 valandas, kreipiasi į paslaugos teikėją ir aiškinasi sutrikimo priežastis ir jų pašalinimo terminus. Nustačius, kad sutrikimas negali būti pašalintas per 4 valandų laikotarpį, Bendrovė kliento tapatybę gali nustatyti pati (pavyzdžiui, fiziškai identifikuoti klientą) arba nukreipti klientus į kito paslaugų teikėjo, teikiančio tapatybės nustatymo paslaugas, sistemą.
- 13.5. Visais atvejais, sutrikus paslaugų teikėjų veiklai, Bendrovės vadovas nedelsiant, visų pirma, turi įvertinti, ar Bendrovė turi technines galimybes ir pasirengimą paslaugų teikėjų teikiamas paslaugų perimti ir vykdyti vidiniais resursais (pavyzdžiui, įvertinti galimybes dalies klientų tapatybę nustatyti fiziškai jiems dalyvaujant ar teisės aktų leidžiamu nuotoliniu būdu ir pan.), jeigu tokias paslaugas Bendrovė turi teisę teikti (pvz., reikėtų atsižvelgti į tai, kad Bendrovė neturi teisės teikti mokėjimo paslaugų).
- 13.6. Jeigu Bendrovė neturi techninių galimybių perimti paslaugų teikėjų teikiamas paslaugas arba neturi teisės teikti atitinkamų paslaugų, Bendrovės vadovas kreipiasi į alternatyvų paslaugos teikėją ir siekia

kaip įmanoma greičiau, bet ne vėliau kaip per 48 valandas sudaryti sutartį dėl atitinkamų paslaugų teikimo.

- 13.7. Rizikos atžvilgiu Bendrovė vertina, kad paslaugų teikėjų veiklos sutrikimų tikimybė yra žema, tačiau tokių sutrikimų neigiamų padarinių lygis gali būti aukštas.

14. REAGAVIMO IR ATKŪRIMO PLANŲ RENGIMAS

- 14.1. Bendrovė, vadovaudamasi poveikio savo veiklai analize, rengia reagavimo ir atkūrimo planus, kuriuose numatoma, kokiomis sąlygomis jie yra taikomi ir kokių veiksmų reikia imtis siekiant užtikrinti kritinių Bendrovėje įdiegtų informacinių ir ryšių technologijų sistemų ir paslaugų prieinamumą, tęstinumą ir atkūrimą.
- 14.2. Bendrovė savo reagavimo ir atkūrimo planuose numato trumpalaikius ir ilgalaikius atkūrimo scenarijus, įvertinant alternatyvas, kai trumpalaikis atkūrimas gali būti neįmanomas dėl sąnaudų, rizikos, logistikos ar kitų nenumatytų aplinkybių.
- 14.3. Bendrovės rengiamiems reagavimo ir atkūrimo planams, be kita ko, taikytini šie reikalavimai:
- 14.3.1. planai rengiami atsižvelgiant į Bendrovės kritinių veiklos funkcijų, pagalbinių procesų, informacinių išteklių ir jų tarpusavio priklausomybės ryšių atkūrimą, siekiant išvengti neigiamo poveikio Bendrovės veiklai ir finansų sistemai;
 - 14.3.2. planai yra užregistruojami bei Bendrovės darbuotojams sudaromos galimybės lengvai juos pasiekti nenumatytu atveju;
 - 14.3.3. planai yra atnaujinami atsižvelgiant į patirtį, sukauptą įvykus incidentams ir atliekant testavimus, nustatytą riziką ir grėsmes, pasikeitusius atkūrimo tikslus ir prioritetus;
 - 14.3.4. planuose yra numatomos tęstinumo priemonės, švelninančios trečiųjų šalių, kurios yra itin svarbios Bendrovės informacinių ir ryšių technologijų paslaugų tęstinumui, veiklos sutrikimus.
- 14.4. Už tinkamą šio skyriaus nuostatų įgyvendinimą yra atsakingas Bendrovės vadovas.

15. MOKUMO PROBLEMOS, BANKROTO RIZIKA AR KITOS PRIEŽASTYS, DĖL KURIŲ BENDROVĖ NEGALI TĖSTI SAVO VEIKLOS

- 15.1. Jeigu Bendrovė susiduria su nekontroliuojamomis mokumo problemomis, Bendrovei iškyla reali bankroto rizika ar atsiranda kitos aplinkybės, dėl kurių Bendrovė negali tinkamai vykdyti savo veiklos, Bendrovė:
- 15.1.1. apie šią situaciją nedelsiant informuoja Lietuvos banką (priežiūros instituciją), detalizuodama esamą rizikos lygį, pasitelktas ar planuojamas pasitelkti rizikos valdymo priemonės bei veiklos tęstinumą užtikrinančias priemones;
 - 15.1.2. nedelsiant atšaukia Platformoje paskelbtus Projektus, kuriems renkamas finansavimas, taip pat nebesudaro ir nebesuteikia galimybės sudaryti naujų sutelktinio finansavimo sandorių (tokių Finansuotojų lėšos yra grąžinamos atgal šiems Finansuotojams);
 - 15.1.3. nedelsiant ieško kito subjekto, galinčio vykdyti sutelktinio finansavimo platformos operatoriaus funkcijas teisės aktuose nustatyta tvarka. Platformos administravimo perdavimas kitam subjektui, turinčiam teisę administruoti sutelktinio finansavimo platformą, jokia būdu negali pabloginti Bendrovės klientų (Finansuotojų ir Projektų savininkų) padėties.
- 15.2. Projektų savininkai ir Finansuotojai sutelktinio finansavimo sandorius (paskolos sutartis) Platformoje sudaro tarpusavyje. Todėl net ir tais atvejais, kai Bendrovė nebegali vykdyti sutelktinio finansavimo platformos operatoriaus veiklos, Projektų savininkai privalės toliau tinkamai vykdyti iš sudarytų sutelktinio finansavimo sandorių (paskolų sutarčių) kylančias savo prievolės Finansuotojams. Bendrovė tokiu atveju:
- 15.2.1. Finansuotojams perduoda turimą informaciją apie jų sudarytus sutelktinio finansavimo sandorius (paskolų sutartis) bei jų vykdymo eigą. Tokiu būdu sudaromos sąlygos

Finansuotojams patiems tiesiogiai vykdyti savo suteiktų paskolų Projektų savininkams administravimą bei išieškojimo procesus;

- 15.2.2. informuoja Projektų savininkus, jog sudarytų ir vykdomų sutelktinio finansavimo sandorių (paskolų sutarčių) administravimą toliau Finansuotojų vardu vykdys ne Bendrovė, o patys Finansuotojai (ar jų paskirtas kitas subjektas). Projektų savininkams suteikiama informacija, reikalinga tam, kad savo įsipareigojimus jie galėtų vykdyti tiesiogiai Finansuotojams.

16. KONTAKTINIAI ASMENYS

- 16.1. Bendrovė patvirtina ir darbuotojams pateikia sąrašą kontaktinių asmenų, su kuriais turi būti nedelsiant susisiekiama įvykus konkrečiam Bendrovės veiklos sutrikimui. Bendrovės darbuotojams identifikavus bet kurį Bendrovės veiklos sutrikimą, be atitinkamame sąrašė nurodytų kontaktinių asmenų, visais atvejais nedelsiant informuojamas Bendrovės vadovas.
- 16.2. Įvykus konkrečiam Bendrovės veiklos sutrikimui, Bendrovės vadovas turi nedelsdamas apie tai informuoti Bendrovės klientus (Finansuotojus ir Projektų savininkus) ir (ar) kitus suinteresuotus asmenis.
- 16.3. Pasikeitus kontaktinių asmenų duomenims, Bendrovės vadovas nedelsiant atnaujina kontaktinių asmenų sąrašė pateiktą informaciją ir su ja Bendrovės nustatyta tvarka supažindina visus Bendrovės darbuotojus.

17. BAIGIAMOSIOS NUOSTATOS

- 17.1. Bendrovės darbuotojai Bendrovės nustatyta tvarka supažindinami su šiame Plane numatytais jų funkcijomis ir pareigomis. Už darbuotojų supažindinimą su Planu atsakingas Bendrovės vadovas.
- 17.2. Bendrovės vadovas yra atsakingas už periodinį (bent kartą per metus) Plano testavimą ir atnaujinimą. Testavimų rezultatai turi būti dokumentuoti, o visi per testavimus nustatyti trūkumai išnagrinėti bei pašalinti.
- 17.3. Planas patvirtinamas, atnaujinamas ar keičiamas Bendrovės vadovo įsakymu.
- 17.4. Planas ir (ar) jo atnaujinimai, pakeitimai įsigalioja kitą dieną nuo jų priėmimo dienos, jeigu nėra nurodyta kita įsigaliojimo data.