Patvirtinta
UAB „Sutelktinio finansavimo platformos „Profitus“
Direktorės 2020 m. balandžio 6 d. įsakymu Nr. 7-2004-3

_____

VEIKLOS TĘSTINUMO PLANAS

1. BENDROSIOS NUOSTATOS

1.1. UAB „Sutelktinio finansavimo platforma „Profitus“ (toliau – **Bendrovė**) veiklos tęstinumo plano (toliau – **Planas**) tikslas yra nustatyti priemones ir procedūras, skirtas užtikrinti Bendrovės nenutrūkstamą veikimą ir paslaugų teikimą esant nenumatytoms situacijoms, už Plano įgyvendinimą atsakingus asmenis.
1.2. Plane vartojamos sąvokos suprantamos taip, kaip jos apibrėžtos pačiame Plane bei Lietuvos Respublikos sutelktinio finansavimo įstatyme.
1.3. Planas yra privalomas visiems Bendrovės darbuotojams.
1.4. Planas yra parengtas vadovaujantis Lietuvos Respublikos sutelktinio finansavimo įstatymu ir kitais teisės aktais.
1.5. Jei kontekstas nereikalauja kitaip, šiame Plane didžiosiomis raidėmis vartojami žodžiai ir išsireiškimai turi žemiau nurodytas reikšmes:
1.5.1. **Finansuotojas** – asmuo, teikiantis Projekto savininkui sutelktinio finansavimo lėšas;
1.5.2. **Įstatymas** – Lietuvos Respublikos sutelktinio finansavimo įstatymas;
1.5.3. **Platforma** – Bendrovės administruojama informacinė sistema, per kurią vykdoma sutelktinio finansavimo veikla, t. y. per kurią Projektų savininkai gali pateikti Paraiškas dėl Projekto finansavimo, kurioje skelbiami finansavimui atrinkti Projektai, per kurią Finansuotojai gali skirti lėšų Projektui, taip pat kurioje skelbiama visa Projektų savininkams ir Finansuotojams svarbi informacija, atliekami kiti sutelktinio finansavimo veiksmai;
1.5.4. **Priežiūros institucija** – Lietuvos bankas;
1.5.5. **Projektas** – verslo, profesinėms, mokslo, tiriamosioms ir kitoms reikmėms, išskyrus vartojimą, tenkinti parengtas ir Platformoje paskelbtas projektas, kuriam įgyvendinti Projekto savininkas siekia pritraukti sutelktinio finansavimo lėšų;
1.5.6. **Projekto savininkas** – asmuo, kuris inicijuoja ir per Platformą paskelbia projektą investuotojams;
1.5.7. **Vadovas** – Bendrovės direktorius (-ė) ar jo įgaliotas asmuo.

2. ORGANIZACINĖS NUOSTATOS

2.1. Įvykus įvykiui ar incidentui (nenumatytai situacijai), kuris ženkliai pakenkė ar gali pakenkti Bendrovės veiklos procesams, įvykį pastebėjęs darbuotojas turi nedelsdamas informuoti Vadovą ar kitą jo įgaliotą asmenį.
2.2. Įvykus įvykiui ar incidentui, Vadovas ne vėliau kaip per 1 valandą nuo įvykio ar incidento paaiškėjimo momento, sudaro Veiklos tęstinumo valdymo grupę, kuri atlieka Veiklos tęstinumo valdymo veiksmus, arba paskiria pagal Planą veikiantį asmenį; jeigu nėra galimybės sudaryti grupės arba paskirti atsakingo asmens, pagal Planą veikiančiu asmeniu laikomas Vadovas (toliau visi šie asmenys vadinami Veikiančiais asmenimis).
2.3. Veikiantys asmenys:
2.3.1. analizuoja įvykius ir incidentus, priima sprendimus veiklos atstatymo ir tęstinumo valdymo klausimais;
2.3.2. bendrauja su viešosios informacijos rengėjų/ skleidėjų atstovais;
2.3.3. bendrauja su teisėsaugos ir kitomis institucijomis;
2.3.4. užtikrina informacijos saugumą įvykus incidentui;
2.3.5. teikia ataskaitas Vadovui apie veiklos tęstinumo valdymą;
2.3.6. vykdo kitas pavestas funkcijas.
2.4. Veikiantys asmenys tarpusavyje bendrauja telefonu, elektroniniu paštu ir/ ar vidine Bendrovės komunikacijos programa.
2.5. Spręsdamas nenumatytas situacijas, Bendrovė remiasi savo darbuotojų žiniomis ir kompetencija informacijos apdorojimo ir ryšių priemonėmis (duomenimis, serverių ir kompiuterių programinėmis ir aparatine įranga, kompiuterių ir telefonų tinklų instaliacija ir aktyvia įranga), Bendrovės techninių priemonių

valdymą ir priežiūrą atliekančios įmonės darbuotojais bei turimomis techninėmis priemonėmis, taip pat, esant poreikiui, ir trečiųjų asmenų paslaugomis.
2.6. Tipiniai reagavimo į nenumatytą situaciją veiksmai yra šie:
2.6.1. įvertinama patirta žala, priimamas sprendimas dėl veiklos tęstinumo plano inicijavimo, įspėjami Bendrovės darbuotojai, Finansuotojai ir Projektų savininkai;
2.6.2. atliekami neatidėliotini veiksmai, užtikrinantys veiklos procesų tęsimą avariniu režimu;
2.6.3. vykdomas kritinių veiklos procesų atstatymas, trunkantis ne ilgiau nei 24 valandas;
2.6.4. pašalinama nenumatyta situacija;
2.6.5. nustatomos/ pašalinamos įvykio/ incidento priežastys;
2.6.6. incidentas fiksuojamas Operacinių įvykių žurnale;
2.6.7. diegiamos prevencijos priemonės.
2.7. Įvykus incidentui maksimalus galimų prarasti duomenų kiekis – paskutinių 24 val. duomenys. Šie duomenys apima visas per šį laikotarpį atliktas vartotojų (Projektų savininkų, Finansuotojų) operacijas.
2.8. Bendrovė kritiniais procesais laiko:
2.8.1. galimybę klientams prisijungti prie savo Finansuotojo ir/ar Projekto savininko paskyros Platformoje;
2.8.2. pagrindinės informacijos (turimos paskolos, lėšų likučiai, suteiktų paskolų portfelis) atvaizdavimą Finansuotojo ir/ar Projekto savininko paskyroje;
2.8.3. pagrindinių operacijų (finansuotis ir finansuoti) vykdymą Finansuotojui ir/ar Projekto savininkui.
2.9. Būdai, priemonės ir veiksmai, naudojami Planui vykdyti, turi būti adekvatūs konkrečiai situacijai.
2.10. Būdai, priemonės ir veiksmai, naudojami Planui vykdyti, turi būti efektyvūs kaštų prasme ir didinti tiesioginę arba netiesioginę ekonominę naudą.
2.11. Visi incidentai, susiję su Bendrovės veiklos tęstinumu, turi būti registruojami Bendrovės Operacinių įvykių žurnale.

3. PAGRINDINĖS BENDROVĖS VEIKLOS RIZIKOS

3.1. Pagrindinės rizikos, galinčios daryti įtaką Bendrovės veiklai yra:
3.1.1. Bendrovės patalpų praradimas;
3.1.2. Bendrovės darbuotojų praradimas;
3.1.3. techninių, duomenų perdavimo priemonių, sistemų, Platformos sutrikimai ir gedimai;
3.1.4. duomenų nutekėjimas (socialinės inžinerijos atakos);
3.1.5. ryšio paslaugų, elektros sutrikimai;
3.1.6. mokėjimo paslaugų partnerių sutrikimai;
3.1.7. tapatybės nustatymo partnerių sutrikimai;
3.1.8. konfidencialių duomenų atskleidimas;
3.1.9. Bendrovės išbraukimas iš Viešojo sutelktinio finansavimo platformų sąrašo;
3.1.10. Bendrovės nemokumas (bankrotas ar restruktūrizavimas) ar veiklos nutraukimas;
3.1.11. ekstremalios situacijos ar karantino paskelbimas.

4. PATALPŲ PRARADIMO ĮVYKIO VALDYMAS

4.1. Patalpos gali būti prarandamos laikinai (negalėjimas patekti į patalpas, pastato laikina evakuacija, elektros, ryšio sutrikimai patalpose, kt.) arba ilgam laikui/ nuolat (nuomos sutarties nutraukimas, gaisras, stichinė nelaimė, teroro aktas, kt.). Vykdant Planą turi būti atsižvelgiama į patalpų praradimo priežastį ir nuolatinumą.
4.2. Rizika dėl patalpų praradimo valdoma imantis prevencinių priemonių, taip pat ją prisiimant.
4.3. Patalpų praradimo įvykio valdymu siekiamas tikslas: užtikrinti darbo ir paslaugų teikimo vietą darbuotojams ir klientams, nenutrūkstamą paslaugų teikimą klientams.
4.4. Prevencijos priemonės:
4.4.1. pasirenkamos tinkamas saugumo priemones turinčios patalpos (veikianti priešgaisrinės apsaugos sistema, praėjimo kontrolė, vaizdo kameros, kt.);
4.4.2. pasirenkamas patikimas patalpų nuomotojas;
4.4.3. tinkamai sudaromi teisiniai dokumentai dėl patalpų nuomos (numatomi nutraukimo terminai, pareigos ir atsakomybės, kitos Bendrovės veiklos tęstinumui būtinos nuostatos);
4.4.4. darbuotojai apmokomi priešgaisrinio saugos taisyklių, saugaus elgesio darbe;
4.4.5. siekiant išvengti Bendrovės dokumentų fizinio praradimo ar sunaikinimo, Bendrovės veikloje naudojami dokumentai, kurie yra esminiai Bendrovės veiklai ir/ar paslaugų teikimui, turi būti skanuojami ir

saugomi elektroniniu būdu Bendrovės serveriuose, Bendrovės kasdienei veiklai naudojami dokumentai turi būti saugomi taip, kad prie jų prieiti galėtų tik tam įgalioti asmenys. Esant poreikiui, Bendrovės veiklos dokumentai gali būti perduodami archyvui;
4.4.6. darbuotojams darbui suteikiami nešiojamieji kompiuteriai, taip pat sukuriama galimybė dirbti nuotoliniu būdu (nuotolinės prieigos).
4.5. Atsakas:
4.5.1. maksimalus atkūrimo laikas iki kritinės situacijos: 24 val.;
4.5.2. jeigu dėl patalpų praradimo kyla grėsmė žmonių gyvybei, sveikatai, turtui (kaip antai, gaisras, stichinė nelaimė, teroro aktas ir pan.), pirmiausia turi būti vykdoma žmonių evakuacija iš patalpų;
4.5.3. nedelsiant yra informuojami už serverių ir IT priežiūrą atsakingi asmenys (dėl nuotolinio darbo organizavimo, reikalingų darbo priemonių, kt.) bei reikiamos avarinės tarnybos (priešgaisrinės apsaugos tarnyba, policija, kt.) bei paslaugų teikėjai;
4.5.4. veikiantys asmenys priima sprendimą dėl tolimesnių veiksmų, reikalingų veiklos procesams tęsti ir imasi priemonių siekiant išvengti Bendrovės dokumentų fizinio praradimo, įvertina patirtą žalą;
4.5.5. techninės priemonės ir ryšiai, elektros tiekimas atstatomi pagal Plano 6 ir 8 skyrius;
4.5.6. Bendrovei praradus patalpas, Vadovas turi organizuoti Bendrovės darbą nuotoliniu būdu arba darbą iš laikinų patalpų (pvz., bendradarbystės erdvių);
4.5.7. jeigu patalpos buvo apgadintos, Vadovas organizuoja patalpų remontą;
4.5.8. jeigu patalpos buvo prarastos visam laikui arba ilgesniam nei vieno mėnesio laikui – Vadovas organizuoja naujų patalpų Bendrovės veiklai suradimą ir veiklos į jas perkėlimą. Iki to laiko dirbama nuotoliniu būdu arba iš laikinų patalpų.

5. DARBUOTOJŲ PRARADIMO ĮVYKIO VALDYMAS

5.1. Bendrovė gali prarasti vieną ar ženklią dalį darbuotojų, taip pat svarbias funkcijas vykdančius darbuotojus, laikinai (dėl ligos, laikino nedarbingumo) ar nuolat. Vykdant Planą turi būti atsižvelgiama į darbuotojo funkcijas, prarandamų darbuotojų kiekį, praradimo priežastį ir nuolatinumą.
5.2. Rizika dėl darbuotojų praradimo valdoma: imantis prevencinių priemonių, taip pat ją prisiimant.
5.3. Darbuotojų praradimo įvykio valdymu siekiamas tikslas: užtikrinti nenutrūkstamą paslaugų teikimą klientams.
5.4. Prevencinės priemonės:
5.4.1. Bendrovės procesai, naudojami įrankiai ir priemonės dokumentuojami, aprašomos procedūros periodinių ar galimai pasikartojančių veiksmų atlikimui tam, kad pasikeitus darbuotojui, naujam darbuotojui būtų pateiktas aiškus vykdomų funkcijų procesas ir aprašymas;
5.4.2. darbuotojai visus darbinius dokumentus turi kelti į Bendrovės vidaus failų serverį, kad išėjus darbuotojui nedingtų veiklai svarbūs dokumentai;
5.4.3. per Platformą su klientais (Finansuotojais, Projektų savininkais) sudaromi dokumentai saugomi Platformoje, o fiziškai arba nuotoliniu būdu ne per Platformą sudaromi dokumentai – saugomi originaliai fiziškai ir Bendrovės vidaus failų serveryje;
5.4.4. visas bendravimas su Bendrovės klientais, partneriais, tiekėjais, kitais asmenimis vyksta tik per darbinėms funkcijoms suteiktas ryšio priemones, kad pasikeitus darbuotojui būtų galima atkurti informaciją ir tęsti bendravimą;
5.4.5. esant galimybei, darbuotojų funkcijos dubliuojamos, t. y. vieno darbuotojo vykdomas funkcijas ar jų dalį turi suprasti ir kitas darbuotojas, kad galėtų pakeisti vienas kitą nedarbingumo, atostogų ar kitais atvejais.
5.5. Atsakas:
5.5.1. maksimalus atkūrimo laikas iki kritinės situacijos: 1–7 darbo dienos;
5.5.2. Bendrovės darbuotojų praradimo atveju, visų pirma, įvertinama patirta žala, jei tokia būtų. Vadovas įvertina, ar: personalo praradimas gali daryti įtaką Bendrovės veiklos vykdymui; kokias prarasto personalo funkcijas būtų galima perduoti kitam Bendrovės darbuotojui; ar yra poreikis priimti kitą darbuotoją (-us) atlikti prarasto personalo funkcijas;
5.5.3. Bendrovės Vadovas paskiria prarasto darbuotojo funkcijas kitam darbuotojui arba prisiima jas vykdyti pats;
5.5.4. esant skubiam personalo poreikiui, Vadovas ieško alternatyvų (pavyzdžiui, paslaugos įsigijimo iš trečiųjų asmenų, darbuotojų nuomos) tol, kol bus surastas reikiamas personalas;
5.5.5. esant poreikiui pakeisti prarastą darbuotoją, Vadovas skelbia naujo darbuotojo atranką.

6. TECHNINIŲ, DUOMENŲ PERDAVIMO PRIEMONIŲ, SISTEMŲ, PLATFORMOS SUTRIKIMŲ IR GEDIMŲ ĮVYKIŲ VALDYMAS

6.1. Techninių, duomenų perdavimo priemonių, sistemų, Platformos sutrikimai ir gedimai gali atsirasti tiek dėl tyčinių trečiųjų asmenų veiksmų (pvz., kibernetinės atakos, dDos atakos, kt.), tiek dėl sistemose, Platformoje esančių klaidų ar netyčinių veiksmų (pvz., interneto sutrikimai, IT sistemų ar programinės įrangos sutrikimai). Vykdant Planą turi būti atsižvelgiama į sutrikimų priežastį, mąstą ir pastebėtą periodiškumą.
6.2. Rizika dėl techninių, duomenų perdavimo priemonių, sistemų, Platformos sutrikimų valdoma: imantis prevencinių priemonių, taip pat ją prisiimant.
6.3. Techninių, duomenų perdavimo priemonių, sistemų, Platformos sutrikimų valdymu siekiamas tikslas: užtikrinti nenutrūkstamą paslaugų teikimą klientams, duomenų saugumą, duomenų ir informacijos atstatymą bei tinkamą sistemų ir kitų priemonių veikimą.
6.4. Prevencinės priemonės:
6.4.1. Bendrovės visų duomenų bazių atsarginės kopijos daromos: pridedamoji kopija – kiekvieną dieną, pilna kopiją kiekvieną – savaitę. Nustačius duomenų sugadinimo momentą, sugadinti duomenys iš duomenų masyvų pakeičiami paskutiniais turimais gerais duomenimis. Tokiu būdu siekiama užtikrinti, kad nenumatytų aplinkybių atveju Bendrovės duomenų bazių įrašai būtų visa ar didžiąja dalimi atstatyti;
6.4.2. Bendrovė duomenis laiko nuotoliniuose duomenų centruose, kurie sertifikuoti pagal ISO 27001 standartus, turi Tier III sertifikatą;
6.4.3. iš klientų (Finansuotojų, Projektų savininkų), Bendrovės darbuotojų reikalaujamas padidintas slaptažodžių sudėtingumas (mažiausiai 8 simboliai su skaičiumi, specialiu simbolius ir/ ar bent viena mažąja ir didžiąja raidėmis), reikalavimas juos keisti reguliariai;
6.4.4. Bendrovė naudojamas virtualus serveris vidinių dokumentų saugojimui atitinka ISO 27001 ir ISO 27018 standartus;
6.4.5. Bendrovės informacinės sistemos kuriamos pagal saugos ir kūrimo gerąsias praktikas.
6.5. Atsakas:
6.5.1. maksimalus atkūrimo laikas iki kritinės situacijos: 24 val. Siekiama, kad maksimalus prarandamas duomenų kiekis būtų ne didesnis nei 24 val. duomenų;
6.5.2. nedelsiant pranešama apie įvykį IT administratoriui, programuotojų funkcijas atliekančiam asmeniui, serverių (duomenų bazių) paslaugų teikėjui;
6.5.3. po 1,5 val.: pranešama klientams apie laikinus sistemos nesklandumus;
6.5.4. jei klaida susijusi su programiniu kodu, vykdomas kodo bazės atstatymas į praėjusią veikiančią versiją;
6.5.5. jei klaida susijusi su prarastais duomenimis, vykdomas duomenų atstatymas į paskutinę turimą versiją;
6.5.6. taisomos klaidos ar kiti sutrikimai;
6.5.7. taisomos saugumo spragos.
6.6. Bendrovė siekia, kad sutrikimų atveju būtų imamasi visų protingų priemonių sumažinti prarandamą duomenų kiekį ir per Plane nurodytus terminus atnaujinti Platformos veiklą.
6.7. Vadovo sprendimu techninių priemonių valdymas, priežiūra, informacijos apdorojimo sistemų priežiūra bei jų veiklos tęstinumo užtikrinimas gali būti perduotas kitam juridiniam asmeniui, kuris privalo užtikrinti jam priskirtų funkcijų tinkamą vykdymą ir Bendrovės paslaugų, sistemų ir infrastruktūros veiklos tęstinumą. Už tai, kad parinktas juridinis asmuo sistemų ir infrastruktūros veiklos tęstinumo neužtikrina arba tai vykdo netinkamai, atsako Vadovas.

7. DUOMENŲ NUTEKĖJIMAS (SOCIALINĖS INŽINERIJOS ATAKOS)

7.1. Bendrovės duomenims gali kilti grėsmė dėl socialinės inžinerijos veiksmų, kai duomenys gali būti prarandami, atskleidžiami ar apribojamas jų pasiekiamumas.
7.2. Bendrovė, siekdama apriboti socialinės inžinerijos atakų galimą riziką, yra patvirtinusi Informacijos saugumo tvarkos aprašą, kuriame aprašyti reikalavimai darbui su Bendrovės įranga, sistemomis, duomenimis. Bendrovėje taip pat vykdomas Bendrovės darbuotojų mokymas informacijos saugumo klausimais.
7.3. Pagrindiniai socialinės inžinerijos grėsmių valdymo būdai:
7.3.1. Užvesti pelės žymeklį ant nuorodos ir patikrinti, ar atvaizduojamas interneto svetainės adresas yra tikras, įsitikinti, kad adrese nėra įvelta gramatinių klaidų, adreso pavadinimas logiškas ir lengvai perskaitomas;
7.3.2. Įsitikinti, kad sesija su interneto svetaine yra šifruojama, t. y. yra naudojamas SSL sertifikatas (interneto svetainės adresas turi prasidėti „https“ žyma), naudoti kelių faktorių autentifikavimo įrankius (pavyzdžiui, slaptažodis, mobilusis įrenginys, piršto antspaudas);

7.3.3. Saugoti savo prisijungimo slaptažodžius, jokiais būdais nelaikyti jų atviru tekstu darbo vietoje, kompiuteryje ar mobiliajame telefone;
7.3.4. Kritiškai vertinti reklamas internete ir elektroniniu paštu siunčiamuose laiškuose (ypač siūlomas dideles nuolaidas). Prašymus atlikti pinigines perlaidas tikrinti kitais būdais, pavyzdžiui, pasitikslinti aplinkybes paskambinus telefonu;
7.3.5. Neatidarinėti dokumentų turinio, siunčiamų failų ir PĮ, kurie yra atsiųsti ar parsisiųsti iš nepatikimo šaltinio (pavyzdžiui, iš nelegalios PĮ platinimo šaltinių).
7.3.6. Neatlikti skubotų veiksmų, nepasiduoti emocijoms, iki galo išsiaiškinti veiksmų, kuriuos prašoma atlikti, būtinumą.
7.4. Bendrovės darbuotojas, pastebėjęs galimą socialinės inžinerijos atakos atvejį, nedelsdamas informuoja apie jį Bendrovės vadovą ir imasi protingų veiksmų, kad tokius veiksmus sustabdytų (pvz., neįleidžia neįgaliotų asmenų į patalpas ir pan.).
7.5. Apie įvykį nedelsiant informuojamos atsakingos institucijos.
7.6. Atsakas:
7.6.1. išsiaiškinama, kaip buvo pažeistas saugumas;
7.6.2. nustatoma nutekėjusi informacija;
7.6.3. taisoma saugumo spraga;
7.6.4. blokuojamos paskyros, kurių prisijungimo duomenys galėjo būti atskleisti dėl spragos;
7.6.5. keičiami prisijungimo duomenys prie partnerių paskyrų;
7.6.6. klientams pranešama apie laikinus sistemos sutrikimus, jei dėl keitimo laikinai apribojamos sistemos funkcijos;
7.6.7. pranešama klientams, jei spraga galėjo atskleisti klientų privačius duomenis;
7.6.8. ruošiamas teisminis ieškinys trečiajai šaliai, kreipiamasi į ikiteisminio tyrimo institucijas.

8. RYŠIO PASLAUGŲ IR ELEKTROS SUTRIKIMŲ ĮVYKIŲ VALDYMAS

8.1. Rizika dėl ryšio paslaugų ir elektros sutrikimų valdoma: imantis prevencinių priemonių, taip pat ją prisiimant.
8.2. Elektros ir ryšio sutrikimų įvykio valdymu siekiamas tikslas: užtikrinti darbo ir paslaugų teikimo vietą darbuotojams ir klientams, nenutrūkstamą paslaugų teikimą klientams.
8.3. Prevencinės priemonės:
8.3.1. biuro patalpos nuomojamos pastate, kuris turi išplėtotą elektros tiekimo infrastruktūrą;
8.3.2. sudaryta galimybė biuro patalpose pajungti mobilų internetą;
8.3.3. darbuotojams darbui suteikti nešiojamieji kompiuteriai, sukurti prisijungimai darbui nuotoliniu būdu, kad darbuotojai savo funkcijas galėtų atlikti ne iš Bendrovės patalpų.
8.4. Atsakas:
8.4.1. maksimalus atkūrimo laikas iki kritinės situacijos: 48 val.
8.4.2. nedelsiant kontaktuojama su biuro pastato administratoriumi dėl elektros sutrikimų, o su interneto tiekėju, dėl interneto sutrikimų;
8.4.3. esant ryšio sutrikimui – pajungiamas mobilus interneto ryšys;
8.4.4. po 2 val. – kontaktuojama su elektros tinklais tiesiogiai, organizuojamas darbuotojų nuotolinis darbas;
8.4.5. po 48 val. nuo elektros sutrikimo: ieškoma (laikinų) biuro patalpų, neturinčių elektros sutrikimų ir/ ar ieškomas naujos interneto paslaugų teikėjas;
8.5. Interneto sutrikimai neturi įtakos Bendrovės duomenų centrų, serverių darbui (Bendrovės nuomojami serveriai yra duomenų centre).

9. MOKĖJIMO PASLAUGŲ, TAPATYBĖS NUSTATYMO PASLAUGŲ PARTNERIŲ SUTRIKIMŲ ĮVYKIŲ VALDYMAS

9.1. Mokėjimo paslaugas, kliento asmens tapatybės nustatymo paslaugas teikiantys partneriai gali nutraukti veiklą, nutraukti bendradarbiavimą su Bendrove ir/ ar Projekto savininku, ar gali sutrikti jų paslaugų teikimas. Vykdant Planą turi būti atsižvelgiama į sutrikimų priežastį, mąstą ir nuolatinumą.
9.2. Rizika dėl mokėjimo paslaugų, tapatybės nustatymo paslaugų partnerių sutrikimų valdoma: imantis prevencinių priemonių, taip pat ją prisiimant.
9.3. Mokėjimo paslaugų, tapatybės nustatymo paslaugų partnerių sutrikimų valdymu siekiamas tikslas: nenutrūkstamas paslaugų teikimas klientams.

9.4. Bendrovė, siekdama išvengti veiklos sutrikimų dėl Partnerių veiklos, imasi tokių prevencinių priemonių:
9.4.1. Bendrovė sudaro sutartis su keliais paslaugų partneriais, kad esant sutrikimams galėtų paslaugų teikimą perkelti į kitą partnerį;
9.4.2. Bendrovė dalį partnerių teikiamų paslaugų gali perimti vykdyti pati.
9.5. Atsakas:
9.5.1. maksimalus atkūrimo laikas iki kritinės situacijos: 24 val.;
9.5.2. sutrikus partnerio veiklai, pirmiausia yra kreipiamasi į partnerį ir aiškinamasi sutrikimo priežastis ir jų pašalinimo terminus;
9.5.3. po 1,5 val. apie sutrikimus informuojami klientai.
9.5.4. nustačius, kad sutrikimas negali būti pašalintas per kelių valandų laikotarpį, Bendrovė:
9.5.4.1. sutrikus Projekto savininko sąskaitą administruojančio paslaugų teikėjo veiklai: surenkamus mokėjimus, esant galimybei, nukreipia į kito mokėjimo paslaugų partnerio įstaigoje atidarytą sąskaitą, skirtą Projekto lėšoms rinkti, arba informuoja Finansuotojus ir prašo jų pateikti finansuojamos sumos mokėjimo pavedimo kopiją, kad galėtų sekti surenkamų sutelktinio finansavimo lėšų sumas;
9.5.4.2. jeigu Projekto savininko sąskaitą administruojančio paslaugų teikėjo veikla sutriko išmokant sumas Finansuotojams, Bendrovė reikalauja, kad Projekto savininkas sumas Finansuotojams išmokėtų iš kitos savo mokėjimo sąskaitos ir pateiktų Bendrovei tai patvirtinančius įrodymus;
9.5.4.3. sutrikus Platformoje integruotam įmokų surinkimo partneriui, Finansuotojai informuojami apie tai, kad investuojamas sumas Projektui turėtų pervesti tiesiogiai į Projekto savininko sąskaitą;
9.5.4.4. sutrikus kliento tapatybę padedančio nustatyti partnerio veiklai, Vadovas ar jo įgaliotas asmuo pirmiausia kreipiasi į Partnerį ir aiškinasi sutrikimo priežastis ir jų pašalinimo terminus. Nustačius, kad sutrikimas negali būti pašalintas per kelių valandų laikotarpį, Bendrovė kliento tapatybę gali nustatyti pati (fizinis kliento identifikavimas).

10. KONFIDENCIALIŲ DUOMENŲ ATSKLEIDIMO ĮVYKIŲ VALDYMAS

10.1. Konfidencialūs duomenys gali būti atskleisti tiesiogiai darbuotojų, taip pat įsilaužiant į Bendrovės sistemas, duomenų bazes, kitais būdais. Vykdant Planą turi būti atsižvelgiama į konfidencialumo pažeidimo priežastį ir mąstą.
10.2. Rizika dėl konfidencialių duomenų atskleidimo valdoma: imantis prevencinių priemonių, taip pat ją prisiimant.
10.3. Konfidencialių duomenų atskleidimo valdymu siekiamas tikslas: užtikrinti klientų duomenų saugumą, užtikrinti nenutrūkstamą paslaugų teikimą.
10.4. Prevencinės priemonės:
10.4.1. Bendrovė veiklą vykdo saugiose, atskirose patalpose, į kurias patekimas yra apribotas tik įgaliotiems asmenims, praėjimas galimas tik su magnetine individualia praėjimo priemone, patekimas į patalpas stebimas vaizdo kameromis;
10.4.2. Bendrovė reikalauja Paslaugų teikėjų užtikrinti, jog pašalinių asmenų patekimas į patalpas, kur saugomos Bendrovės tarnybinės stotys, serveriai, neįmanomas, o įgaliotų asmenų patekimas yra ribojamas, labai griežtai tikrinamas bei fiksuojamas; patekimas galimas tik su lydinčiu asmeniu;
10.4.3. Bendrovė reikalauja Paslaugų teikėjų užtikrinti, jog patalpos, kuriose yra Bendrovės serveriai, yra rakinamos su dviejų lygių prieigos kontrole, naudojamos mechaninės ir elektroninės spynos, įrengtas apsaugos postas, patalpos stebimos vaizdo kameromis.
10.4.4. darbuotojams yra vykdomi periodiniai saugumo mokymai;
10.4.5. vykdomas įdarbinamų darbuotojų reputacijos patikrinimas;
10.4.6. sistemose naudojamos specializuotos ugniasienės ir įsilaužimo aptikimo sistema;
10.4.7. kompiuteriuose diegiama naujausia antivirusinė programa;
10.4.8. vykdoma prieigos teisių ir rolių kontrolė, fiksuojami naudotojų veiksmai sistemose;
10.4.9. iš sistemų naudotojų reikalaujamas padidintas slaptažodžių sudėtingumas (mažiausiai 8 simboliai su skaičiumi, specialiu simbolius ir/ ar bent viena mažąja ir didžiąja raidėmis), reikalavimas juos keisti reguliariai;
10.4.10. Bendrovė duomenis laiko nuotoliniuose duomenų centruose, kurie atitinka ISO 27001 standartus;
10.4.11. Bendrovė naudojamas virtualus serveris vidinių dokumentų saugojimui atitinka ISO 27001 ir ISO 27018 standartus;
10.4.12. siekiant apsaugoti sistemą nuo kibernetinių atakų, duomenų nuskaitymo, visa informacija nuotoliniu būdu gali būti pasiekiama tik naudojant šifruotą komunikacijos kanalą, t. y. kriptografinius protokolus (pvz., TLS, SSL).

10.5. Atsakas:
10.5.1. maksimalus atkūrimo laikas iki kritinės situacijos: 24 val.;
10.5.2. nedelsiant pranešama apie įvykį IT administratoriui, programuotojų funkcijas atliekančiam asmeniui, serverių (duomenų bazių) paslaugų teikėjui;
10.5.3. aiškinamasi, kaip buvo pažeistas saugumas;
10.5.4. nustatoma atskleista informacija;
10.5.5. taisomos saugumo spragos;
10.5.6. jeigu duomenys buvo atskleisti dėl darbuotojo veiksmų – apribojamas darbuotojo patekimas į Bendrovės patalpas ir prisijungimas prie sistemų;
10.5.7. blokuojamos paskyros, kurių prisijungimo duomenys galėjo būti atskleisti dėl spragos;
10.5.8. keičiami prisijungimo duomenys prie partnerių paskyrų;
10.5.9. klientams pranešama apie laikinus sistemos sutrikimus, jei dėl keitimo laikinai apribojamos sistemos funkcijos;
10.5.10. pranešama klientams, jei spraga galėjo atskleisti klientų privačius duomenis;
10.5.11. ruošiamas teisminis ieškinys trečiajai šaliai, kreipiamasi į ikiteisminio tyrimo institucijas;
10.5.12. pakeičiami prisijungimo duomenys visose sistemose vietoj atskleistų.
10.5.13. įvertinamos galimybės apsisaugoti nuo analogiškų atakų ateityje.

11. BENDROVĖS IŠBRAUKIMAS IŠ VIEŠOJO SUTELKTINIO FINANSAVIMO PLATFORMŲ SĄRAŠO ĮVYKIŲ VALDYMAS

11.1. Bendrovė gali būti išbraukiama iš Viešojo sutelktinio finansavimo platformų sąrašo teisės aktų nustatyta tvarka.
11.2. Rizika dėl Bendrovės išbraukimo iš Viešojo sutelktinio finansavimo platformų sąrašo valdoma: ją prisiimant.
11.3. Bendrovės išbraukimo iš Viešojo sutelktinio finansavimo platformų sąrašo valdymu siekiamas tikslas: užtikrinti klientų interesų apsaugą.
11.4. Atsakas:
11.4.1. nedelsiant po išbraukimo iš sąrašo, Bendrovė nebeleidžia sudaryti naujų Finansavimo sandorių;
11.4.2. išbraukus Bendrovę iš sutelktinio finansavimo platformų sąrašo, per 48 darbo valandas apie šį sprendimą yra informuojami Bendrovės klientai (Finansuotojai ir Projektų savininkai);
11.4.3. jau sudaryti Finansavimo sandoriai yra vykdomi toliau, t. y. priimamos įmokos ir palūkanos iš Projekto savininkų ir paskirstomos Finansuotojams, išskyrus atvejus, kai šie įsipareigojimai teisės aktų nustatyta tvarka yra perduoti kitiems asmenims;
11.4.4. tais atvejais, kai prašymą išbraukti iš sutelktinio finansavimo platformų sąrašo pateikia pati Bendrovė, ji turi būti sudariusi susitarimą su kitu sutelktinio finansavimo platformos operatoriumi dėl finansavimo sandorių administravimo perdavimo. Tokiu atveju klientai per 48 darbo valandas po Bendrovės išbraukimo iš sutelktinio finansavimo platformų operatorių sąrašo informuojami apie naują jų paslaugų teikėją, atsiskaitymų vykdymo tvarką;
11.4.5. Bendrovė siekia užtikrinti, kad Bendrovės platformos administravimas būtų sklandžiai perduodamas kitam subjektui, t. y. kad neatsirastų Platformos veiklos sutrikimų.
11.5. Bendrovės išbraukimo iš viešojo sutelktinio finansavimo operatorių sąrašo atveju už tinkamą Bendrovės įsipareigojimų vykdymą yra atsakingas Vadovas ar jo įgaliotas asmuo.

12. BENDROVĖS NEMOKUMO (ĮSKAITANT BANKROTO IR RESTRUKTŪRIZAVIMO ATVEJUS) AR VEIKLOS NUTRAUKIMO ĮVYKIŲ VALDYMAS

12.1. Rizika dėl nemokumo valdoma: taikant prevencines priemones, ją prisiimant.
12.2. Nemokumo atveju siekiamas tikslas: užtikrinti klientų interesų apsaugą.
12.3. Prevencinės priemonės:
12.3.1. Finansuotojų ir Projektų savininkų lėšos yra laikomos atskirai nuo Bendrovės turto, t. y. jos yra renkamos į specialią sąskaitą ir į ją grąžinamos. Todėl Bendrovės nemokumo atveju Bendrovės kreditoriai neturėtų galimybės tenkinti savo reikalavimų iš Bendrovės klientų turto.
12.4. Atsakas:
12.4.1. per 48 darbo valandas po nemokumo sprendimo įsiteisėjimo dienos, apie šį sprendimą yra informuojami Bendrovės klientai (Finansuotojai ir Projektų savininkai);

12.4.2. nedelsiant stabdoma naujų Finansuotojų registracija, naujų paskolų išmokėjimas ir Projektų savininkų paraiškų priėmimas, Finansavimo sandorių sudarymas;
12.4.3. jau sudaryti Finansavimo sandoriai yra vykdomi toliau, t. y. įmokos ir palūkanos iš Projekto savininkų toliau skirstomos Finansuotojams iš Projekto savininkų vardu atidarytų sąskaitų; išskyrus atvejus, kai šie įsipareigojimai teisės aktų nustatyta tvarka yra perduoti kitiems asmenims;
12.4.4. Vadovas bendradarbiauja su Priežiūros institucija ir paskirtu Bendrovės administratoriumi siekiant efektyvaus Platformos administravimo ar jo perdavimo, Projekto finansavimo atšaukimo iš Platformos.
12.5. Bendrovei bankrutuojant ar vykdant restruktūrizaciją, jau sudaryti Finansavimo sandoriai yra laikomi galiojančiais ir privalo būti šalių vykdomi toliau. Finansavimo sandorių (įskaitant įkeitimo sandorius) administravimas toliau vykdomas administratoriaus arba teisės aktų nustatyta tvarka perduodamas tretiesiems asmenims.
12.6. Už tinkamą Bendrovės pareigų vykdymą bankroto ar restruktūrizavimo atveju yra atsakingas Vadovas ir/ ar administratorius.
12.7. Investuotojų ir Projektų savininkų lėšos yra laikomos atskirai nuo Bendrovės turto. Todėl Bendrovės nemokumo atveju Bendrovės kreditoriai neturėtų galimybės tenkinti savo reikalavimų iš Bendrovės klientų turto.

13. EKSTREMALIOS SITUACIJOS AR KARANTINO PASKELBIMAS

13.1. Ekstremali situacija ar karantinas skelbiamas Lietuvos Respublikos vyriausybės nutarimu;
13.2. Ekstremalios situacijos ar karantino paskelbimo metu siekiama užtikrinti nenutrūkstamą paslaugų teikimą klientams.
13.3. Prevencijos priemonės:
13.3.1. darbuotojams darbui suteikiami nešiojamieji kompiuteriai, taip sukuriama galimybė dirbti nuotoliniu būdu (nuotolinės prieigos);
13.3.2. pasirenkamos tinkamas saugumo priemones turinčios patalpos (veikianti priešgaisrinės apsaugos sistema, praėjimo kontrolė, vaizdo kameros, kt.);
13.3.3. vykdoma švietimo veiklą, skirtą sukurti veiklos tęstinumo procesų sampratai bei užtikrinti, kad procesai būtų efektyvūs;
13.3.4. nuolatos atnaujinamos procedūros, kurios nustato kokių reikia imtis veiksmų grįžtant į normalų veiklos ritmą;
13.3.5. nuodugnus pasirengimas (tikrinimas siekiant nustatyti, ar organizacija, personalas, įranga, priemonės ir procedūros gali susidoroti su darbu ekstremalios situacijos ar karantino sąlygomis).
13.4. Atsakas:
13.4.1. Bendrovės vadovas priima sprendimą dėl tolimesnių veiksmų, reikalingų veiklos procesams tęsti ir imasi priemonių siekiant išvengti Bendrovės bankroto/nemokumo, darbuotojų praradimo bei įvertina patirtą žalą;
13.4.2. Bendrovės darbas nedelsiant organizuojamas nuotoliniu būdu;
13.4.3. klientai aptarnaujami taip pat nuotoliniu būdu, išskyrus atvejus, kai būtina atitinkamas funkcijas atlikti tam tikroje vietoje (notarų biuras, VĮ Registrų centras ir kt.);
13.4.4. projektų savininkai bei Investuotojai nuolatos informuojami apie esamą situaciją;
13.4.5. užtikrinama, kad ir toliau būtų tinkamai atskleidžiama situacija, reikalinga investuotojams ir kitiems rinkos dalyviams, kad jie galėtų laiku ir tinkamai įvertinti savo investicijas ir priimti teisingus ir pagrįstus sprendimus;
13.4.6. atsižvelgiant į situaciją koreguojamas paskolų rizikos vertinimo algoritmas;
13.4.7. vykdoma sutelktų paskolų bei mokėjimo terminų peržiūra;
13.4.8. periodiškai siunčiami pranešimai apie būsimus palūkanų bei paskolų mokėjimus.

14. BAIGIAMOSIOS NUOSTATOS

14.1. Šis Planas įsigalioja nuo jo patvirtinimo dienos ir gali būti panaikintas ar pakeistas tik Vadovo įsakymu.
14.2. Už tinkamą šio Plano laikymąsi yra atsakingas Vadovas ar kitas jo paskirtas asmuo.
14.3. Popierinė Plano kopija yra saugoma Bendrovės patalpose, o elektroninė – Bendrovės serveryje.
14.4. Bendrovės darbuotojai turi būti supažindinti su Planu ir jame numatytomis jų pareigomis.
14.5. Planas turi būti skelbiamas platformoje.

14.6. Vadovo įgaliotas asmuo ne rečiau nei kartą per 12 mėnesių atlieka Plano tikrinimo procedūrą – testavimą, kurio metu nustatoma, ar Planas būtų tinkamai vykdomas susiklosčius nenumatytai situacijai. Bandymo metu Bendrovės paskirti atsakingi darbuotojai išanalizuoja galimą (sumodeliuotą) saugos incidentą, numato galimus jo valdymo būdus ir sprendimus.
14.7. Išbandžius Plano veiksmingumą, atsakingi darbuotojai parengia Valdymo plano veiksmingumo išbandymo ataskaitą.
14.8. Išbandymo metu pastebėti trūkumai šalinami remiantis operatyvumo, veiksmingumo ir ekonomiškumo principais.
14.9. Šis Planas yra peržiūrimas esant poreikiui, tačiau ne rečiau nei kas 2 metus.