

PATVIRTINTA

UAB „Finansų bitė“

Direktoriaus įsakymu Nr. 1-0804/2020

UAB „FINANSŲ BITĖ“ VEIKLOS TĘSTINUMO PLANAS

1. BENDROSIOS NUOSTATOS

- 1.1. Tarpusavio skolinimo operatoriaus UAB „Finansų bitė“ (toliau – Bendrovė) veiklos tęstinumo plane (toliau – Planas) nustatomi reikalavimai, siekiant numatyti priemones ir procedūras, skirtas užtikrinti, kad Bendrovės funkcijos būtų atliekamos nenutrūkstamai, įskaitant ir nenumatytų aplinkybių atvejus, o tipinis reagavimas į nenumatytą situaciją būtų detaliai aptartas.
- 1.2. Šis Planas yra tvirtamas Bendrovės direktoriaus (toliau – Vadovas) ir įsigalioja nuo jo patvirtinimo dienos. Šiuo Planu savo veikloje vadovaujasi visi Bendrovės darbuotojai.

2. PAGRINDINĖS BENDROVĖS VEIKLOS RIZIKOS

- 2.1. Pagrindinės rizikos, galinčios daryti įtaką Bendrovės veiklai:
 - 2.1.1. Bendrovės patalpų ar su jomis susijusių paslaugų praradimas;
 - 2.1.2. Duomenų praradimo rizika;
 - 2.1.3. Technologijų rizika;
 - 2.1.4. Personalo rizika;
 - 2.1.5. Trečiųjų šalių rizika;
 - 2.1.6. Atitikties rizika
 - 2.1.7. Tapatybės nustatymo partnerių sutrikimai;
 - 2.1.8. Duomenų nutekėjimas;
 - 2.1.9. Ekstremalios situacijos ar karantino paskelbimas;
 - 2.1.10. Likvidumo rizika;

3. BENDROVĖS PATALPŲ AR SU JOMIS SUSIJUSIŲ PASLAUGŲ PRARADIMAS

- 3.1. 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.). Vykdam Planą turi būti atsižvelgiama į patalpų praradimo priežastį ir nuolatinumą. Taip pat galimas elektros, interneto ar kitų darbui būtinų ryšių praradimas.
- 3.2. Rizika dėl patalpų praradimo valdoma imantis prevencinių priemonių, taip pat ją prisiimant.
- 3.3. Patalpų praradimo įvykio valdymu siekiamas tikslas: užtikrinti darbo ir paslaugų teikimo vietą darbuotojams ir klientams, nenutrūkstamą paslaugų teikimą klientams.
- 3.4. Prevencijos priemonės:

- 3.4.1. pasirenkamos tinkamas saugumo priemonės turinčios patalpos (veikianti priešgaisrinės apsaugos sistema, praėjimo kontrolė, vaizdo kameros, kt.);
- 3.4.2. pasirenkamas patikimas patalpų nuomotojas;
- 3.4.3. tinkamai sudaromi teisiniai dokumentai dėl patalpų nuomos (numatomi nutraukimo terminai, pareigos ir atsakomybės, kitos Bendrovės veiklos tęstinumui būtinos nuostatos);
- 3.4.4. siekiant išvengti Bendrovės dokumentų fizinio praradimo ar sunaikinimo, Bendrovės veikloje naudojami dokumentai, kurie yra esminiai Bendrovės veiklai ir/ar paslaugų teikimui, turi būti skenuojami 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;
- 3.4.5. darbuotojams darbui suteikiami nešiojamieji kompiuteriai, taip pat sukuriama galimybė dirbti nuotoliniu būdu (nuotolinės priegijos).
- 3.4.6. biuro patalpos nuomojamos pastate, kuris turi išplėtotą elektros tiekimo infrastruktūrą;
- 3.4.7. sudaryta galimybė biuro patalpose naudoti mobilųjį internetą;
- 3.5. maksimalus atkūrimo laikas iki kritinės situacijos: 24 val.;
- 3.6. 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;
- 3.7. 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;
- 3.8. veikiantys asmenys priima sprendimą dėl tolimesnių veiksmų, reikalingų veiklos procesams tęsti ir imasi priemonių siekiant išvengti Bendrovės dokumentų fizinio praradimo, įvertinta patirtą žalą;
- 3.9. nedelsiant kontaktuojama su biuro pastato administratoriumi dėl elektros sutrikimų, o su interneto tiekėju, dėl interneto sutrikimų. Maksimalus atkūrimo laikas – 48 valandos.
- 3.10. po 48 val. nuo elektros sutrikimo: ieškoma (laikinių) biuro patalpų, neturinčių elektros sutrikimų ir/ ar ieškomas naujos interneto paslaugų teikėjas. Iki tol naudojamas mobilusis internetas, kontaktuojama su elektros bei interneto tiekėjais, esant reikalui – organizuojamas nuotolinis darbas;
- 3.11. Bendrovei praradus patalpas, Vadovas turi organizuoti Bendrovės darbą nuotoliniu būdu arba darbą iš laikinų patalpų (pvz., bendradarbystės erdvių);
- 3.12. jeigu patalpos buvo apgadintos, Vadovas organizuoja patalpų remontą;
- 3.13. 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.

4. DUOMENŲ PRARADIMO RIZIKA

- 4.1. Klientai, naudodamiesi Bendrovės informacine sistema, generuoja ir saugo didelius kiekius duomenų, įskaitant ir jautrią asmeninę informaciją. Pagrindiniai duomenų praradimo rizikos faktoriai yra šie:
 - 4.1.1. Duomenų praradimas arba sugadinimas;
 - 4.1.2. Duomenų vagystė, neteisėtas pakeitimas ar panaudojimas.
- 4.2. Šiame Plane, Bendrovės patvirtintoje Saugumo politikoje, Prieigų valdymo tvarkoje, Saugumo incidentų valdymo tvarkoje yra apibrėžti technologiniai sprendimai, nustatyti atsakingi Bendrovės asmenys bei aprašytos procedūros, kuriomis Bendrovės darbuotojai savo veikloje

- vadovaujasi, siekiant sumažinti iki minimalaus priimtino lygio nurodytų duomenų rizikos faktorių tikimybę bei poveikį, įvykus su šiais faktoriais susijusiam incidentui.
- 4.3. Pagrindiniai įsilaužimo (duomenų praradimo kibernetinės atakos atveju) grėsmių valdymo būdai:
 - 4.3.1.[KONFIDENCIALU];
 - 4.3.2.[KONFIDENCIALU];
 - 4.3.3.[KONFIDENCIALU];
 - 4.3.4.[KONFIDENCIALU];
 - 4.3.5.[KONFIDENCIALU];
 - 4.3.6.[KONFIDENCIALU].
 - 4.4. Bendrovės darbuotojas, pastebėjęs galimą kibernetinės atakos atvejį, nedelsdamas informuoja apie jį Bendrovės vadovą ir imasi protingų veiksmų, kad tokius veiksmus sustabdytų (pvz., neįleidžia neįgaliotų asmenų į patalpas ir pan.).
 - 4.5. Apie įvykį nedelsiant informuojamos atsakingos institucijos.
 - 4.6. išsiaiškinama, kaip buvo pažeistas saugumas;
 - 4.7. nustatoma nutekėjusi informacija;
 - 4.8. taisoma saugumo spraga;
 - 4.9. blokuojamos paskyros, kurių prisijungimo duomenys galėjo būti atskleisti dėl spragos;
 - 4.10. keičiami prisijungimo duomenys prie partnerių paskyrų;
 - 4.11. klientams pranešama apie laikinus sistemos sutrikimus, jei dėl keitimo laikinai apribojamos sistemos funkcijos;
 - 4.12. pranešama klientams, jei spraga galėjo atskleisti klientų privačius duomenis;
 - 4.13. ruošiamas teisminis ieškinys trečiajai šaliai, kreipiamasi į ikiteisminio tyrimo institucijas

5. TECHNOLOGIJŲ RIZIKA

- 5.1. Bendrovės veikloje naudojama techninė ir programinė įranga dėl natūralaus nusidėvėjimo, įrangos gamyklinių arba įdiegimo klaidų gali nustoti veikti arba imti veikti neteisingai. Taip pat galimi tyčiniai trečiųjų šalių veiksmai (kibernetinės atakos). Bendrovė naudoja šias priemones iki minimalaus priimtino lygio sumažinančias šį techninės ir programinės įrangos rizikos faktorių:
 - 5.1.1.[KONFIDENCIALU].
 - 5.1.2.Įranga yra pilnai dubliuota, t. y. sugedus vienam Įrangos vienetui toliau veikia kitas Įrangos vienetas, atliekantis tą pačią funkciją, taip pat įranga yra dubliuojama duomenis saugant ir kitur esančiuose serveriuose (debesijos paslauga);
 - 5.1.3.Įrangoje veikiantys programiniai komponentai (aplikacijos, duomenų bazės) savo ruožtu taip pat yra dubliuoti, t. y. sugedus vienam programiniam komponentui toliau veikia kita komponento kopija, atliekanti tą pačią funkciją;
 - 5.1.4.Bendrovės už naudojamos sistemos valdymą paskirtas atsakingas darbuotojas, t. y. Sistemos administratorius, nuolat seka informaciją apie pasirodžiusius ar atskleistus programinės įrangos komponentų (operacinės sistemos, aplikacijos, duomenų bazės, tinklo programinės įrangos, papildomos sisteminės programinės įrangos) pažeidžiamumus ir užtikrina tokios programinės įrangos ar jos komponentų versijų atnaujinimą arba saugumo pataisų (angl. *security patches*) neatidėliotą ištestavimą ir įdiegimą.
- 5.2. Bendrovės visų duomenų bazių atsarginės kopijos daromos: pridedamoji kopija – kiekvieną dieną, pilna kopija - kiekvieną savaitę. Nustačius duomenų sugadinimo momentą, sugadinti duomenys iš duomenų masyvų pakeičiami paskutiniais turimais gerais duomenimis. Tokiu

- būdu siekiama užtikrinti, kad nenumatyty aplinkybių atveju Bendrovės duomenų bazių įrašai būtų visa ar didžiąja dalimi atstatyti;
- 5.3. Bendrovė duomenis laiko nuotoliniuose duomenų centruose, kurie sertifikuoti pagal ISO 27001 standartus, turi Tier III sertifikatą.
 - 5.4. maksimalus atkūrimo laikas iki kritinės situacijos: 24 val. Siekiama, kad maksimalus prarandamas duomenų kiekis būtų ne didesnis nei 24 val. duomenų;
 - 5.5. nedelsiant pranešama apie įvykį IT administratoriui, programuotojų funkcijas atliekančiam asmeniui, serverių (duomenų bazių) paslaugų teikėjui;
 - 5.6. po 1,5 val.: pranešama klientams apie laikinus sistemos nesklaidumus;
 - 5.7. jei klaida susijusi su programiniu kodu, vykdomas kodo bazės atstatymas į praėjusią veikiančią versiją;
 - 5.8. jei klaida susijusi su prarastais duomenimis, vykdomas duomenų atstatymas į paskutinę turimą versiją;
 - 5.9. taisomos klaidos ar kiti sutrikimai;
 - 5.10. taisomos saugumo spragos.
 - 5.11. Bendrovė siekia, kad sutrikimų atveju būtų imamasi visų protingų priemonių sumažinti prarandamą duomenų kiekį ir per Plane nurodytus terminus atnaujinti Bendrovės veiklą.
 - 5.12. 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.

6. PERSONALO RIZIKA

- 6.1. Žmogiškųjų išteklių ir (ar) kompetencijų trūkumo bei darbuotojų praradimo Bendrovėje (personalo) rizika yra valdoma šiomis priemonėmis:
 - 6.1.1. Bet kurioje Bendrovės veiklos proceso grandyje yra bent du darbuotojai, galintys atlikti tą pačią funkciją ir turintys tam reikiamas kompetencijas;
 - 6.1.2. Bendrovė darbuotojų sukauptą patirtį ir žinias fiksuoja ir jomis dalinasi per vidinę žinių valdymo informacinę sistemą (*KONFIDENCIALU*);
 - 6.1.3. Bendrovė nuolat investuoja į darbuotojų mokymąsi, jų kompetencijų plėtrą ir naujų kompetentingų darbuotojų pritraukimą.
 - 6.1.4. 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;
 - 6.1.5. darbuotojai visus darbinius dokumentus turi kelti į Bendrovės vidaus failų serverį, kad išėjus darbuotojui nedingtų veiklai svarbūs dokumentai;
 - 6.1.6. 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;
- 6.2. maksimalus atkūrimo laikas iki kritinės situacijos: 1–7 darbo dienos;
- 6.3. Bendrovės darbuotojų praradimo atveju, visų pirma, įvertinama patirta žala, jei tokia būtų. Vadovas įvertina, ar personalo praradimas gali daryti įtaką Bendrovės veiklos vykdymui:
 - 6.3.1. kokias prarasto personalo funkcijas būtų galima perduoti kitam Bendrovės darbuotojui;
 - 6.3.2. ar yra poreikis priimti kitą darbuotoją (-us) atlikti prarasto personalo funkcijas;

- 6.3.3. Bendrovės Vadovas paskiria prarasto darbuotojo funkcijas kitam darbuotojui arba prisiima jas vykdyti pats;
- 6.3.4. esant skubiam personalo poreikiui, Vadovas ieško alternatyvų (pavyzdžiui, paslaugos įsigijimo iš trečiųjų asmenų, darbuotojų nuomos) tol, kol bus surastas reikiamas personalas;
- 6.3.5. esant poreikiui pakeisti prarastą darbuotoją, Vadovas skelbia naujo darbuotojo atranką.

7. TREČIŲJŲ ŠALIŲ RIZIKA

- 7.1. Prieš pasirenkant trečiąją šalį kaip paslaugų tiekėją ar subtiekęją atliekama šios trečiosios šalies rizikos analizė ir vertinimas.
- 7.2. Atliekant trečiosios rizikos vertinimą vadovaujama tokiais pačiais kriterijais kuriais Bendrovė įsipareigoja prieš savo Klientus bei galiojančiais atitikties reikalavimais finansinių institucijų kritinių funkcijų paslaugų tiekėjams.
- 7.3. Trečiajai šaliai neatitikus reikalavimų keliamų rizikos vertinime, pasiūloma ištaisyti trūkumus per abipusiai priimtą laikotarpį. Trūkumų neištaisius, paslaugos teikimo sutartis su trečiaja šalimi nepasirašoma, arba atitinkama galiojanti sutartis nutraukiama pagal joje aprašytas sąlygas.
- 7.4. Paslaugų teikimo sutartys pasirašomos tik su tomis trečiosiomis šalimis, kurių įvertinta rizika atitinka Bendrovei priimtą lygį bei įsipareigojimus Klientams.
- 7.5. Trečiųjų šalių rizikos vertinimą bei kriterijų peržiūrą atlieka Bendrovės darbuotojas, atsakingas už Bendrovės atitiktį nustatytiems reikalavimams (jei paskirtas), ir (ar) Bendrovės direktorius ne rečiau kaip kartą per metus visoms trečioms šalims, su kuriomis Bendrovė turi galiojančias paslaugų teikimo sutartis.

8. ATITIKTIES RIZIKA

- 8.1. Bendrovės veikla yra prižiūrima Lietuvos banko (toliau - Priežiūros institucija), kas užtikrina galimų veiklos neatitikimų teisės aktams identifikavimą anksčiau nei atsiranda pažeidimas bei užkerta kelią tolimesniems pažeidimams.
- 8.2. Bendrovės įstatuose numatyta trijų pakopų valdymo sistema. Veikia šie valdymo organai: visuotinis akcininkų susirinkimas, valdyba, Bendrovės direktorius. Bet kuriam vienam iš valdymo organų neatliekant jam teisės aktais bei Bendrovės įstatais priskirtų funkcijų, šios funkcijos atlikimą gali perimti kitas organas. Jei atitinkamos funkcijos perėmimas nėra leidžiamas teisės aktu, valdyba apie tai informuojama ir teikia pasiūlymą visuotiniam akcininkų susirinkimui. Tokia valdymo sistema užtikrina, kad visos teisės aktų nustatytos funkcijos būtų atliekamos tinkamai ir laiku.
- 8.3. Bendrovėje yra paskirtas Atitikties specialistas, atsakingas už teisinės bei atitikties rizikų vertinimą, bendravimą su priežiūros institucijomis, atitikties užtikrinimą Bendrovėje.

9. TAPATYBĖS NUSTATYMO PARTNERIŲ SUTRIKIMAI

- 9.1. Kliento asmens tapatybės nustatymo paslaugas teikiantys partneriai gali nutraukti veiklą, nutraukti bendradarbiavimą su Bendrove, gali sutrikti jų paslaugų teikimas. Vykdam Planą turi būti atsižvelgiama į sutrikimų priežastį, mastą ir nuolatinumą.
- 9.2. Rizika dėl tapatybės nustatymo paslaugų partnerių sutrikimų valdoma: imantis prevencinių priemonių, taip pat ją prisiimant.

- 9.3. tapatybės nustatymo paslaugų partnerių sutrikimų valdymu siekiamas tikslas - nenutrūkstamas paslaugų teikimas klientams.
- 9.4. Bendrovė, siekdama išvengti veiklos sutrikimų dėl Partnerių veiklos, dalį partnerių teikiamų paslaugų gali perimti vykdyti pati.
- 9.5. maksimalus atkūrimo laikas iki kritinės situacijos: 24 val.;
- 9.6. sutrikus partnerio veiklai, pirmiausia yra kreipiamasi į partnerį ir aiškinamasi sutrikimo priežastis ir jų pašalinimo terminus;
- 9.7. po 1,5 val. apie sutrikimus informuojami klientai.
- 9.8. nustačius, kad sutrikimas negali būti pašalintas per kelis valandų laikotarpį, Bendrovė kliento tapatybę gali nustatyti pati (kliento identifikavimas tiek nuotoliniu būdu, tiek fiziniu).

10. DUOMENŲ NUTEKĖJIMAS

- 10.1. Konfidencialūs duomenys gali būti atskleisti tiesiogiai darbuotojų, taip pat įsilaužiant į Bendrovės sistemas, duomenų bazines, kitais būdais. Vykdamas Planą turi būti atsižvelgiama į konfidencialumo pažeidimo priežastį ir mastą.
- 10.2. Konfidencialių duomenų atskleidimo valdymu siekiamas tikslas: užtikrinti klientų duomenų saugumą, užtikrinti nenutrūkstamą paslaugų teikimą.
- 10.3. Bendrovė veiklą vykdo saugiose, atskirose patalpose, į kurias patekimas yra apribotas tik įgaliotiems asmenims, patekimas į patalpas stebimas vaizdo kameromis;
- 10.4. Bendrovė reikalauja Paslaugų teikėjų užtikrinti, jog [KONFIDENCIALU];
- 10.5. Bendrovė reikalauja Paslaugų teikėjų užtikrinti, jog [KONFIDENCIALU].
- 10.6. darbuotojams yra vykdomi periodiniai saugumo mokymai;
- 10.7. vykdomas įdarbinamų darbuotojų reputacijos patikrinimas;
- 10.8. sistemose naudojamos [KONFIDENCIALU];
- 10.9. kompiuteriuose diegiama naujausia antivirusinė programa;
- 10.10. vykdoma prieigos teisių ir rolių kontrolė, fiksuojami naudotojų veiksmai sistemose;
- 10.11. iš sistemų naudotojų reikalaujamas padidintas slaptažodžių sudėtingumas [KONFIDENCIALU];
- 10.12. Bendrovė duomenis laiko nuotoliniuose duomenų centruose, kurie atitinka [KONFIDENCIALU];
- 10.13. [KONFIDENCIALU].
- 10.14. maksimalus atkūrimo laikas iki kritinės situacijos: 24 val.;
- 10.15. nedelsiant pranešama apie įvykį IT administratoriui, programuotojų funkcijas atliekančiam asmeniui, serverių (duomenų bazių) paslaugų teikėjui;
- 10.16. aiškinamasi, kaip buvo pažeistas saugumas;
- 10.17. nustatoma atskleista informacija;
- 10.18. taisomos saugumo spragos;
- 10.19. jeigu duomenys buvo atskleisti dėl darbuotojo veiksmų – apribojamas darbuotojo patekimas į Bendrovės patalpas ir prisijungimas prie sistemų;
- 10.20. blokuojamos paskyros, kurių prisijungimo duomenys galėjo būti atskleisti dėl spragos;
- 10.21. [KONFIDENCIALU];
- 10.22. klientams pranešama apie laikinus sistemos sutrikimus, jei dėl keitimo laikinai apribojamos sistemos funkcijos;
- 10.23. pranešama klientams, jei spraga galėjo atskleisti klientų privačius duomenis;
- 10.24. ruošiamas teisminis ieškinys trečiajai šaliai, kreipiamasi į ikiteisminio tyrimo institucijas;
- 10.25. pakeičiami prisijungimo duomenys visose sistemose vietoj atskleistų.
- 10.26. įvertinamos galimybės apsaugoti nuo analogiškų atakų ateityje.

11. EKSTREMALIOS SITUACIJOS AR KARANTINO PASKELBIMAS

- 11.1. Ekstremali situacija ar karantinas skelbiamas Lietuvos Respublikos Vyriausybės nutarimu;
- 11.2. Ekstremalios situacijos ar karantino paskelbimo metu siekiama užtikrinti nenutrūkstamą paslaugų teikimą klientams.
- 11.3. darbuotojams darbui suteikiami nešiojamieji kompiuteriai, taip sukuriama galimybė dirbti nuotoliniu būdu (nuotolinės prieigos);
- 11.4. pasirenkamos tinkamas saugumo priemonės turinčios patalpos (veikianti priešgaisrinės apsaugos sistema, praėjimo kontrolė, vaizdo kameros, kt.);
- 11.5. vykdoma švietimo veikla, skirta sukurti veiklos tęstinumo procesų sampratai bei užtikrinti, kad procesai būtų efektyvūs;
- 11.6. nuolatos atnaujinamos procedūros, kurios nustato kokių reikia imtis veiksmų grįžtant į normalų veiklos ritmą;
- 11.7. nuodugnus pasirengimas (tikrinimas siekiant nustatyti, ar organizacija, personalas, įranga, priemonės ir procedūros gali susidoroti su darbu ekstremalios situacijos ar karantino sąlygomis).
- 11.8. 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;
- 11.9. Bendrovės darbas nedelsiant organizuojamas nuotoliniu būdu;
- 11.10. klientai aptarnaujami taip pat nuotoliniu būdu, išskyrus atvejus, kai būtina atitinkamas funkcijas atlikti tam tikroje vietoje (notarų biuras, VĮ Registrų centras ir kt.);
- 11.11. klientai nuolatos informuojami apie esamą situaciją;
- 11.12. užtikrinama, kad ir toliau būtų tinkamai atskleidžiama situacija, reikalinga klientams ir kitiems rinkos dalyviams;
- 11.13. atsižvelgiant į situaciją koreguojamas paskolų rizikos vertinimo algoritmas;
- 11.14. vykdoma paskolų bei mokėjimo terminų peržiūra;
- 11.15. periodiškai siunčiami pranešimai apie būsimus palūkanų bei paskolų mokėjimus.

12. LIKVIDUMO RIZIKA

- 12.1. Rizika, kad Bendrovė nesugebės laiku įvykdyti finansinių įsipareigojimų, pasireiškianti laikinu arba nuolatiniu Bendrovės nemokumu ir kraštutiniu atveju – bankroto bylos Bendrovei iškelimu.
- 12.2. Vadovaujantis Finansų įstaigų įstatymu, Bendrovės bankroto procedūra galėtų būti iškelta tik teismo tvarka. Pareiškimą teismui dėl bankroto bylos iškelimo Bendrovei turi teisę pateikti jos dalyviai, likvidatorius, administracijos vadovas, kreditorius (kreditoriai) ir Lietuvos bankas.
- 12.3. Jeigu pareiškimą teismui dėl bankroto bylos iškelimo pateiktų ne Lietuvos bankas, teismas, prieš priimdamas sprendimą dėl bankroto bylos iškelimo, privalėtų gauti Lietuvos banko išvadą dėl Bendrovės nemokumo.
- 12.4. Ne vėliau nei kitą darbo dieną po pareiškimo teismui dėl bankroto bylos iškelimo, iš karto sužinojus apie jį, ar iki kreditorių susirinkimo dienos, kai siekiama vykdyti bankroto procesą ne teismo tvarka, Vadovas nustato laikiną Investuotojų lėšų, Paskolų gavėjų portfelio, Skolininkų portfelio (toliau – Turto) administravimą ir perduoda Turtą administruoti

laikinajam turto administratoriui. Taip pat gali būti nuspręsta nebeišduoti naujų paskolų ir/ar sustabdyti antrinės rinkos funkcionalumą.

- 12.5. Laikinajam turto administratoriui, pagal iš anksto sudarytą susitarimą, perduodami duomenys, dokumentai ir prisijungimai prie sistemos bei sąskaitų, taip pat perduodamas kontaktų sąrašas;
- 12.6. Laikinajam turto administratoriui taip pat perduodami duomenys apie visas paskolas, sutartis, paskolų gavėjų mokėtinas sumos investuotojams (paskolos davėjams), mokėjimų grafikai, duomenys apie antrinės rinkos sandorius;
- 12.7. Bendrovė apmoko laikinąjį turto administratorių naudotis Bendrovės sistema ir portfelio administravimo įrankiais;
- 12.8. Duomenys apie paskolų portfelį yra atiduodami ir nuolatos atnaujinami į Lietuvos banko ir / arba UAB Creditinfo Lietuva administruojamą įsipareigojimų duomenų bazę;
- 12.9. Laikinas administratorius atskiria Bendrovei ir Investuotojams priklausančias Paskolų portfelio dalis ir lėšas. Laikinas administratorius veda Paskolų gavėjų ir Investuotojų apskaitą. Laikino turto administravimo metu administratorius apskaito Bendrovės ir Investuotojų Turto lėšas atskirose depozitinėse sąskaitose. Taip pat, Laikinas administratorius administruoja nutrauktų paskolų portfelį, ikiteisminius, teismo, vykdymo procesus, bei turi įgaliojimus nutraukti nemokias paskolų sutartis, perduoti skolininkus ikiteisminiam išieškojimui, teismui, bei vykdymui. Išieškotos lėšos laikomos atskirai;
- 12.10. Po Turto perdavimo kuo greičiau, bet ne vėliau nei iki teismo nutarties iškelti Bendrovei bankroto bylą įsiteisėjimo dienos ar kreditorių komiteto nutarimo paskirti bankroto administratorių, jei bankroto procesas vykdomas ne teismo tvarka laikinas administratorius įsipareigoja skelbti ir įvykdyti aukcioną, informaciją apie aukcioną išviešinti informacinėse priemonėse, siūlant įsigyti Paskolų portfelį ir kitą perduotą turtą ir/ar perimti Investuotojų Turto administravimą ir kitų įsipareigojimų naudos gavėjams (Investuotojams) vykdymą. Paskolų portfelio pardavimo aukciono būdu tikslas yra patenkinti kreditorių, kuris (kurie) kreipėsi į teismą dėl bankroto bylos iškėlimo, reikalavimus, ir taip panaikinti aplinkybes, kurios yra/ galėtų būti pagrindas iškelti bankroto bylą Bendrovei pagal ĮBĮ 9(5) ar kreditorių susirinkimui priimti nutarimą vykdyti bankroto procedūras ne teismo tvarka (ĮBĮ 12(4). Veiksmų, dėl Turto (paskolų portfelio) pardavimo, laikinas turto administratorius imasi, kadangi turtas turi finansinę vertę ir jo, priklausomai nuo faktinės situacijos tuo metu, gali pakakti atsiskaityti su kreditoriais ir nutraukti bankroto procesą. Aukciono taisykles ir tvarką nustato Laikinas administratorius. Jis gali paskirti aukciono organizatorių vykdyti aukcioną. Laikinas administratorius gali atskirti Paskolų portfelį (gerosios, blogosios paskolos), ir siūlyti jas aukcione pirkti atskirai, taip pat gali siūlyti aukcione pirkti tik Bendrovei ar tik Investuotojams priklausančias Paskolų portfelio dalis. Investuotojams priklausančio paskolų portfelio ar jo dalies pardavimas galimas, tik jei Investuotojai išreiškia sutikimą (sprendimui pritaria kvalifikuota (2/3) visų elektroninėmis priemonėmis balsavusių (valių išreiškusių), Investuotojų) dėl Turto pardavimo (pvz. veiksmų ir/ar neveiksmų paskolų portfelio dalies). Jei Investuotojų sutikimas dėl Turto pardavimo nėra gaunamas, Laikinas administratorius el. būdu Investuotojams teikia alternatyvius siūlymus. Jei alternatyviu balsavimu sprendimas nėra priimamas, tai Laikinas administratorius rengia trečiąjį ir galutinį balsavimą dėl Investuotojų Turto pardavimo. Šio balsavimo rezultatai yra galutiniai ir laimi daugiausiai balsų surinkęs siūlymas. Šio siūlymo pagrindu yra rengiamas Investuotojų Turto pardavimas aukciono būdu. Aukcione turtas parduodamas aukščiausią kainą pasiūliusiam asmeniui;
- 12.11. Tuo atveju, jei aukcionas neįvyksta, ar lieka turto, kuris nėra realizuotas, Laikinas administratorius pateikia Laikino administratoriaus siūlymus Investuotojams dėl tolimesnių veiksmų, bei išsiunčia pranešimus elektroniniu laišku paskutiniaisiais žinomais Investuotojų el.

pašto adresais. Laikinasis administratorius vykdo apklausą el. būdu. Laikinasis administratorius gali priimti sprendimą skelbti Investuotojų susirinkimą. Investuotojų apklausai, balsavimui, susirinkimui, sprendimų priėmimui pagal analogiją taikomos LR Civilinio Kodekso ir Akcinių bendrovių įstatymo nuostatos. Laikinasis administratorius tariasi su Lietuvos banku ar kitais rinkos dalyviais dėl Paskolų portfelio ar jo dalies perleidimo;

- 12.12. Įsiteisėjus teismo nutarčiai iškelti bankroto bylą ir/ar teismui ar kreditorių komitetui paskyrus bankroto administratorių, laikinasis administratorius perduoda bankroto administratoriui tą Paskolų portfelio (Turto) dalį (lėšas), kurios priklauso Bendrovei, ir kuri galima atskirti nuo Investuotojų turto. Investuotojams priklausantis Paskolų portfelis ir Investuotojų turtas (lėšos) nėra perduodamas (ĮBĮ 10(7)(1)). Bendrovei priklausanti Turta (Paskolų portfelį sudaro įplaukos iš (i) investicijų (paskolos) dalies (grįžtančios Bendrovei, kai Bendrovė yra suteikusi bent dalį bendros vartojimo kredito sumos, arba kai Bendrovė yra suteikusi visą vartojimo kredito sumą); (ii) palūkanų (grįžtančios Bendrovei, kai Bendrovė yra suteikusi bent dalį bendros vartojimo kredito sumos, arba tik Bendrovei, kai Bendrovė yra suteikusi visą vartojimo kredito sumą); (iii) vėlavimo mokesčių (mokėjimo pradelsimo atveju visais atvejais grįžta tiek Investuotojams, tiek Bendrovei, arba tik Bendrovei, kai Bendrovė yra suteikusi visą vartojimo kredito sumą); (iv) kitų mokesčių (Sutarties ir Administravimo mokesčio, kuris visais atvejais mokamas tik Bendrovei); (v) procesinių palūkanų (grįžtančios tiek Investuotojams, tiek Bendrovei. Jei turto neįmanoma atskirti, Laikinasis administratorius perduoda tik Bendrovei priklausančias lėšas, kurias galima atskirti. Jei dėl bankroto administratoriui perduodamo turto apimtys kyla ginčas, jis sprendžiamas teisme civilinio proceso kodekso nustatyta tvarka;
- 12.13. Laikinasis Turto administravimas pasibaigia, anksčiausiai įvykus vienai iš šių sąlygų: (i) Paskolų portfelis yra parduota(s) ar perleistas administruoti kitam asmeniui; (ii) priimamas sprendimas užbaigti laikinąjį administravimą; (iii) įsiteisėja teismo nutartis (sprendimas), kuriame nustatyta laikinojo turto administravimo pabaiga ir sąlygos;
- 12.14. Bankroto administratorius taip pat administruotų tarpusavio skolinimo sandorius ir jų vykdymą, kadangi iškėlus bankroto bylą Bendrovei, tarpusavio skolinimo sandoriai liktų teisiškai galiojantys nepaisant Bendrovės teisinio veiksnio statuso. Šių sandorių pagrindu vartojimo kredito gavėjų mokėtinos sumos priklausytų paskolos davėjams, o bankroto administratorius neturėtų teisių į jokiais Paskolos davėjams priklausančias lėšas, kurias gražintų vartojimo kredito gavėjai.

13. TIPINIS REAGAVIMAS Į NENUMATYTĄ SITUACIJĄ

- 13.1. Bendrovės veiklos tęstinumą planuoja ir valdo Bendrovės direktorius, kuris priima sprendimus dėl:
- 13.1.1. kritinės situacijos paskelbimo, jei neįmanoma incidento suvaldyti pasitelkus Plane numatytas rizikos valdymo priemones;
 - 13.1.2. finansinių ir kitų išteklių, reikalingų greitam Bendrovės veiklos atkūrimui, paieškos ir skyrimo.
- 13.2. Bendrovės duomenų, personalo, trečiųjų šalių, atitikties rizikų atsiradusių incidentų šalinimui valdyti Bendrovės direktorius paskiria atsakingą asmenį (toliau – Administratorius).
- 13.3. Administratoriaus funkcijos, užtikrinant Bendrovės veiklos tęstinumą:
- 13.3.1. situacijos analizė, problemų (incidentų) nustatymas;
 - 13.3.2. įvykusio incidento tyrimo koordinavimas ir bendravimas su kitais incidentų tyrime bei šalinime dalyvaujančiais subjektais;

- 13.3.3. veiklos atkūrimo organizavimas ir koordinavimas Bendrovės vadovui paskelbus kritinę situaciją;
- 13.3.4. sprendimų dėl Bendrovės veiklos tęstinumo valdymo klausimais priėmimas ir įgyvendinimo kontrolė;
- 13.3.5. informacijos apie atsiradusių incidentų ar nenumatytų situacijų sprendimo eigą, veiksmus jiems pašalinti ir rekomendacijų, kaip elgtis, teikimas Bendrovės darbuotojams ir Bendrovės klientams;
- 13.3.6. bendradarbiavimas su kompetentingomis institucijomis;
- 13.3.7. logistikos organizavimas (žmogiškieji ištekliai, daiktai, įranga).
- 13.4. Įvykus incidentui ir (ar) nustačius Bendrovės veiklos sutrikimą, Administratorius informuoja Bendrovės direktorių ir imasi šių veiksmų:
 - 13.4.1. priima sprendimą dėl reikalingų veiksmų incidentui pašalinti ir Bendrovės veiklai atkurti;
 - 13.4.2. nustato incidento padarytą žalą;
 - 13.4.3. jei reikia, atkuria duomenis iš atsarginių kopijų (duomenų ir (ar) technologijų srities incidentas);
 - 13.4.4. informuoja Priežiūros instituciją (jei privaloma).
- 13.5. Sudėtingiems ir svarbiems incidentams spręsti gali būti sudaryta atskira darbo grupė. Darbo grupės sudėtį tvirtina Bendrovės direktorius.

14. BAIGIAMOSIOS NUOSTATOS

- 14.1. Planas turi būti išbandomas vieną kartą per metus arba esant didesniems informacinės sistemos, aplinkos (pvz., patalpų pakeitimas), paslaugų tiekėjų, personalo pokyčiams. Plano išbandymo metu Administratorius (jei paskirtas) ir (ar) Bendrovės direktorius išanalizuoja galimą (sumodeliuotą) kritinę situaciją, numato galimus jos valdymo būdus, galimus sprendimus ir parengia Plano išbandymo ataskaitą.
- 14.2. Planas turi būti peržiūrimas ne rečiau kaip kartą per metus arba po jo išbandymo ir atnaujinamas esant būtinybei.
- 14.3. Už plano peržiūrą ir (ar) atnaujinimą yra atsakingas Administratorius (jei paskirtas) ir (ar) Bendrovės direktorius.