Forma 2.1

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 Bendrovės nenutrūkstamam veikimui ir paslaugų teikimui esant nenumatytoms situacijoms.

1.2. Plane vartojamos sąvokos suprantamos taip, kaip jos apibrėžtos Lietuvos Respublikos sutelktinio finansavimo įstatyme, nebent Plane detalizuojama kitaip.

1.3. Šiuo Planu turi vadovautis Bendrovė.

1.4. Planas yra parengtas vadovaujantis Lietuvos Respublikos sutelktinio finansavimo įstatymu ir jį lydinčiais įgyvendinamaisiais teisės aktais.

2. SĄVOKOS

2.1. Jei kontekstas nereikalauja kitaip, šiame Plane didžiosiomis raidėmis vartojami žodžiai ir išsireiškimai turi žemiau nurodytas reikšmes:

2.1.1. **Bendrovės platforma** – Bendrovės administruojama informacinė sistema, kurią naudojant vykdomas sutelktinis finansavimas.

2.1.2. **Investuotojas** – asmuo, teikiantis projekto savininkui sutelktinio finansavimo lėšas.

2.1.3. **Įstatymas** – Lietuvos Respublikos sutelktinio finansavimo įstatymas.

2.1.4. **Projektas** – verslo, profesinėms, mokslo, tiriamosioms ir kitoms reikmėms, išskyrus vartojimą, tenkinti parengtas ir Bendrovės platformoje paskelbtas projektas, kuriam įgyvendinti Projekto savininkas siekia pritraukti sutelktinio finansavimo lėšų.

2.1.5. **Projekto savininkas** – asmuo, kuris inicijuoja ir per Bendrovės platformą paskelbia projektą investuotojams.

2.1.6. **Vadovas** – Bendrovės direktorius (-ė).

3. ORGANIZACINĖS NUOSTATOS

3.1. 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.

3.2. Įvykus įvykiui ar incidentui, Bendrovės vadovas gali sudaryti Veiklos tęstinumo valdymo grupę, kuri atlieka Veiklos tęstinumo valdymo veiksmus, arba pagal Planą veikia įgaliotas asmuo (toliau visi šie asmenys vadinami Veikiančiais asmenimis). Veikiantys asmenys:

3.2.1. analizuoja įvykius ir incidentus, priima sprendimus veiklos tęstinumo valdymo klausimais;

3.2.2. bendrauja su viešosios informacijos rengėjų/ skleidėjų atstovais;

3.2.3. bendrauja su teisėsaugos ir kitomis institucijomis;

3.2.4. užtikrina informacijos saugumą, įvykus incidentui;

3.2.5. teikia ataskaitas Bendrovės vadovui apie veiklos tęstinumo valdymą;

3.2.6. vykdo kitas pavestas funkcijas.

3.3. Veikantys asmenys tarpusavyje bendrauja telefonu, elektroniniu paštu ir/ ar vidine Bendrovės komunikacijos programa.

3.4. Spręsdama nenumatytą situaciją Bendrovė remiasi savo darbuotojų žiniomis ir kompetencija informacijos apdorojimo ir ryšių priemonėmis (duomenimis, serverių ir kompiuterių programinė ir aparatinė 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.

3.5. Tipiniai reagavimo į nenumatytą situaciją veiksmai yra šie:

3.5.1. įvertinama patirta žala, priimamas sprendimas dėl veiklos tęstinumo plano inicijavimo, įspėjami Bendrovės darbuotojai, Investuotojai ir Projektų savininkai;

3.5.2. atliekami neatidėliotini veiksmai, užtikrinantys veiklos procesų tęsimą avariniu režimu;

3.5.3. vykdomas kritinių veiklos procesų atstatymas, trunkantis ne ilgiau nei 24 valandas;

3.5.4. nenumatytos situacijos pašalinimas;

3.5.5. priežasčių nustatymas/ pašalinimas;

3.5.6. incidento fiksavimas operacinių įvykių žurnale;

3.5.7. prevencijos priemonių diegimas.

3.6. Įvykus incidentui maksimalus galimų prarasti duomenų kiekis – paskutinių 24 val. duomenys. Šie duomenys apima visas per šį laikotarpį atliktas vartotojų operacijas.

3.7. Bendrovė kritiniais procesais laiko:

3.7.1. galimybę vartotojams prisijungti prie savo Investuotojo ir/ar Projekto savininko paskyros Bendrovės platformoje;

3.7.2. pagrindinės informacijos (turimos paskolos, lėšų likučiai, suteiktų paskolų portfelis) atvaizdavimą Investuotojo ir/ar Projekto savininko paskyroje;

3.7.3. pagrindinių operacijų (finansuotis ir finansuoti) vykdymą Investuotojui ir/ar Projekto savininkui.

3.8. Būdai, priemonės ir veiksmai, naudojami Planui vykdyti, turi būti adekvatūs konkrečiai situacijai.

3.9. Būdai, priemonės ir veiksmai, naudojami Planui vykdyti, turi būti efektyvūs kaštų prasme ir didinti tiesioginę arba netiesioginę ekonominę naudą.

3.10. Visi incidentai, susiję su Bendrovės veiklos tęstinumu, turi būti registruojami Bendrovės operacinių įvykių žurnale.

4. PAGRINDINĖS BENDROVĖS VEIKLOS RIZIKOS:

4.1. Pagrindinės rizikos, galinčios daryti įtaką Bendrovės veiklai yra:

4.1.1. Bendrovės patalpų praradimas;

4.1.2. Bendrovės darbuotojų praradimams;

4.1.3. Duomenų perdavimo sutrikimai ir gedimai;

4.1.4. Ryšio paslaugų sutrikimai;

4.1.5. Techninės įrangos gedimai;

4.1.6. Platformos sutrikimai;

4.1.7. Duomenų praradimas/ atskleidimas (socialinės inžinerijos įvykiai);

4.1.8. Mokėjimų, tapatybės nustatymo partnerių sutrikimai;

4.1.9. Bendrovės išbraukimas iš viešojo sutelktinio finansavimo platformų operatorių sąrašo;

4.1.10. Bendrovės nemokumas (bankrotas ar restruktūrizavimas) ar veiklos nutraukimas.

5. BENDROVĖS VEIKLOS ATSTATYMAS PATALPŲ PRARADIMO AR DARBUOTOJŲ PRARADIMO ATVEJU

5.1. Bendrovės patalpų praradimo atveju (gaisro, stichinės nelaimės, teroro akto, nusikalstamų veikų ar kitų veiksmų atveju), visų pirma, vykdoma žmonių evakuacija; Vadovas ar jo įgaliotas asmuo priima sprendimą dėl tolimesnių veiksmų, reikalingų veiklos procesams tęsti, imasi priemonių siekdamas išvengti Bendrovės dokumentų fizinio praradimo, įvertina patirtą žalą; techninės priemonės ir ryšiai atstatomi atsižvelgiant į techninių priemonių valdymo ir priežiūros taisykles, pateiktas 6 skyriuje, nedelsiant yra informuojami už serverių ir IT priežiūrą atsakingi asmenys bei reikiamos avarinės tarnybos.

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

5.3. Vadovas ar jo įgaliotas asmuo, kuris paskirtas atsakingu už Plano vykdymą, privalo užtikrinti, kad, siekiant išvengti Bendrovės dokumentų fizinio praradimo ar sunaikinimo dėl stichinės nelaimės, teroro akto, nusikalstamų veikų ar kitų veiksmų, Bendrovės veikloje naudojami dokumentai, kurie yra esminiai Bendrovės veiklai ir/ar paslaugų teikimui, būtų skanuojami ir saugomi elektroniniu būdu Bendrovės serveriuose, Bendrovės kasdienei veiklai naudojami dokumentai turi būti saugomi rakinamose spintose. Esant poreikiui, Bendrovės veiklos dokumentai gali būti perduodami archyvui.

5.4. Maksimalus atkūrimo laikas patalpų praradimo atveju iki kritinės situacijos: 24 val. Atsakas:

5.4.1. vykdoma evakuacija iš pastato;

5.4.2. pranešama atitinkamoms tarnyboms (priešgaisrinės apsaugos tarnybai, policijai, kt.);

5.4.3. organizuojamas darbuotojų nuotolinis darbas;

5.4.4. esant poreikiui remontuojamos patalpos tinkamai darbo aplinkai užtikrinti ar ieškoma laikinų ar tiesiog naujų patalpų ofisui.

5.5. Bendrovės darbuotojų praradimo atveju, visų pirma, įvertinama patirta žala, jei tokia būtų. Vadovas įvertina, ar:

5.5.1. personalo praradimas gali daryti įtaką Bendrovės veiklos vykdymui;

5.5.2. kokias prarasto personalo funkcijas būtų galima perduoti kitam Bendrovės darbuotojui;

5.5.3. ar yra poreikis priimti kitą darbuotoją (-us) atlikti prarasto personalo funkcijas;

5.5.4. esant skubiam personalo poreikiui, Vadovas ieško alternatyvų (pavyzdžiui, paslaugos įsigijimo iš trečiųjų asmenų, darbuotojų nuomos) tol, kol bus surastas reikiamas personalas. Kol bus pradėtos teikti paslaugos ar įdarbintas darbuotojas, reikiamos vykdyti funkcijos padalinamos tarp kitų Bendrovės darbuotojų.

6. TECHNINIŲ, DUOMENŲ PERDAVIMO, RYŠIO PRIEMONIŲ, PLATFORMOS SUTRIKIMŲ VALDYMAS, PRIEŽIŪRA NENUMATYTOS SITUACIJOS ATVEJU

6.1. Techninių, duomenų perdavimo, ryšio priemonių platformos sutrikimu valdymu ir priežiūra yra siekiama, kad dėl nenumatytų aplinkybių nustojus veikti Bendrovės platformai, sistemoms, duomenų bazėms (interneto sutrikimai, IT sistemų ar programinės įrangos sutrikimai, kibernetinės atakos) valdomi duomenys ir informacija būtų visa ar didžiąja dalimi atstatyti per įmanomai trumpiausią laiką, o po sutrikimų Bendrovės platforma ir sistemos toliau veiktų.

6.2. Už tinkamą šių priemonių priežiūros ir valdymo organizavimą yra atsakingas Bendrovės Vadovas ar jo įgaliotas asmuo, ar trečiasis asmuo, teikiantis tokio pobūdžio paslaugas.

6.3. Bendrovė naudoja šias priemones apsaugai nuo programinės įrangos sugadinimo ir duomenų praradimo:

6.3.1. daromos Bendrovės serveryje esančios informacijos (įskaitant sisteminius aplankus) kopijos. Kiekvieną dieną laikotarpiu nuo 2:00 iki 3:00 val. daromos atsarginės virtualaus serverio kopijos, t. y. kopijuojama visa, kas yra Bendrovės serveryje. Tokiu būdu siekiama užtikrinti,

kad nenumatytų aplinkybių atveju Bendrovės serveryje esantys duomenys būtų visa ar didžiąja dalimi atstatyti;

6.3.2. Bendrovė naudoja ir virtualų serverį, kuris atitinka ISO 27001 ir ISO 27018 standartą;

6.3.3. Bendrovė duomenis laiko nuotoliniuose duomenų centruose, kurie atitinka ISO 27001 standartus.

6.3.4. Bendrovės duomenų bazių kopijos daromos kiekvieną dieną laikotarpiu tarp 23:00 iki 24:00 (dienos kopijos), bei kiekvieno mėnesio 30tą dieną tarp 2:00 ir 3:00 val. (mėnesio kopijos). 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;

6.3.5. Siekiant apsaugoti sistemą nuo kibernetinių atakų, duomenų nuskaitymo, visa informacija pasiekiama panaudojant virtualaus privataus tinklo prisijungimus (VPN). Platformos priežiūros specialistai koduoja slaptažodžius prieš siunčiant juos į duomenų bazę, svarbius veiksmus puslapyje papildomai saugoja slaptažodžio prašymu. Iš vartotojų 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. Bendrovės darbuotojai naudojasi nešiojamais bei stacionariais kompiuteriais (Apple arba analogiškus standartus atitinkančiais), kurie yra prijungti prie Bendrovės serverių. Todėl Bendrovės patalpose esant interneto ryšio sutrikimams, Bendrovės veikla gali būti perkeliama vykdyti į kitas patalpas (pavyzdžiui, namus), o įrangos praradimo atveju yra išsaugoma svarbi informacija. Interneto sutrikimai neturi įtakos Bendrovės duomenų centrų, serverių darbui (Bendrovės nuomojami serveris yra duomenų centre).

6.5. Bendrovė siekia, kad sutrikimų atveju būtų imamasi visų protingų priemonių sumažinti prarandamą duomenų kiekį ir per Plane nurodytus terminus atnaujinti Bendrovės platformos veiklą. Siekiama, kad maksimalus prarandamas duomenų kiekis būtų ne didesnis nei 24 val. duomenų.

6.6. 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. Funkcijų perdavimo atveju tokio juridinio asmens kontaktai pridedami kaip priedas prie šio Plano. Už tai, kad parinktas juridinis asmuo sistemų ir infrastruktūros veiklos tęstinumo neužtikrina arba tai vykdo netinkamai, atsako Bendrovės operacijų vadovas.

6.7. Sutrikus platformos (Bendrovės sistemų) veiklai, pirmiausia turi būti krepiamasi į programavimo paslaugų teikėjus ar vidinius Bendrovės programuotojus ir ieškoma klaidų. Vėliau, jei nustatoma, kad tai nėra programavimo klaidos, kreipiamasi į serverių (duomenų bazių) paslaugų teikėjus.

6.8. Esant ryšio sutrikimui patalpose, Bendrovės vadovo sprendimu gali būti organizuojamas mobilus interneto ryšys.

6.9. Maksimalus atkūrimo laikas iki kritinės situacijos: 24 val. Atsakas:

6.9.1. pagal sutrikimų pobūdį gali būti kreipiamasi į energijos, ryšių ar kitų paslaugų teikėjus;

6.9.2. pranešama programavimo paslaugų teikėjams apie sutrikimus (sutrikimų šalinimo laikas: 2 val.);

6.9.3. pranešama serverių (duomenų bazių) paslaugų teikėjams (sutrikimų šalinimo laikas: 2 val.);

6.9.4. po 2 valandų, neveikiant platformai ar kitiems kritiniams procesams: informuojami klientai;

6.9.5. gali būti organizuojamas darbuotojų nuotolinis darbas.

7. DUOMENŲ NUTEKĖJIMAS (SOCIALINĖS INŽINERIJOS ATAKOS)

7.1. Bendrovės duomenims gali kilti rizika ne vien dėl techninių Bendrovės sistemų, ryšių pažeidimų, bet ir 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. 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.).

7.4. Įvykus tokiam įvykiui, vykdomas tyrimas, siekiant nustatyti pažeidimo priežastį, mastą ir galimas pasekmes.

7.5. Apie įvykį nedelsiant informuojamos ikiteisminio tyrimo institucijos, atsakingi darbuotojai nušalinami nuo darbo.

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. MOKĖJIMŲ, TAPATYBĖS NUSTATYMO PARTNERIŲ SUTRIKIMAI

8.1. Mokėjimas paslaugas, kliento asmens tapatybės nustatymo paslaugas teikiantys partneriai gali nutraukti veiklą, nutraukti bendradarbiavimą su Bendrove ar gali sutrikti jų paslaugų teikimas.

8.2. Bendrovė, siekdama išvengti veiklos sutrikimų dėl Partnerių veiklos, imasi tokių veiksmų:

8.2.1. sudaro sutartis su keliais paslaugų partneriais, kad esant sutrikimams galėtų paslaugų teikimą perkelti į kitą partnerį;

8.2.2. dalį partnerių teikiamų paslaugų gali perimti vykdyti pati.

8.3. Sutrikus mokėjimo paslaugų partneriui, Bendrovės 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 surenkamus mokėjimus, esant galimybei, nukreipia į kito mokėjimo paslaugų partnerio įstaigoje atidarytą Sąskaitą, skirta sutelktinio finansavimo lėšoms administruoti, arba informuoja investuotojus ir prašo jų pateikti investuotos sumos pavedimo kopiją, kad galėtų sekti surenkamų sutelktinio finansavimo lėšų sumas.

8.4. Mokėjimų partneriui užlaikius Investuotojams ar Projekto savininkams mokėtinas lėšas ilgiau nei 24 val., esant poreikiui inicijuojamas Bendrovės papildomas finansavimas, užtikrinant savalaikį atsiskaitymą.

8.5. Sutrikus kliento tapatybę padedančio nustatyti partnerio veiklai, Bendrovės 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) arba nukreipia klientus į kito partnerio, teikiančio tapatybės nustatymo paslaugas, sistemą.

8.6. Atsakas:

8.6.1. nustatomas galimas sutrikimo šalinimo laikas;

8.6.2. apie sutrikimus informuojami klientai;

8.6.3. kliento tapatybės nustatymas, mokėjimų vykdymas nukreipiamas pas kitus paslaugų teikėjus, esant galimybei – vykdomas tiesiogiai.

9. BENDROVĖS IŠBRAUKIMAS IŠ VIEŠOJO SUTELKTINIO FINANSAVIMO PLATFORMŲ OPERATORIŲ SĄRAŠO

9.1. Bendrovė gali būti išbraukiama iš viešojo sutelktinio finansavimo platformų operatorių sąrašo teisės aktų nustatyta tvarka.

9.2. Bendrovę išbraukus iš sutelktinio finansavimo platformų operatorių sąrašo, apie šį sprendimą yra informuojami Bendrovės klientai (Investuotojai ir Projektų savininkai).

9.3. Po išbraukimo iš sąrašo, Bendrovė nebeleidžia sudaryti naujų Finansavimo sandorių. Jau sudaryti Finansavimo sandoriai yra vykdomi toliau, t. y. priimamos įmokos ir Palūkanos iš Projekto savininkų ir paskirstomos Investuotojams; išskyrus atvejus, kai šie įsipareigojimai teisės aktų nustatyta tvarka yra perduoti kitiems asmenims.

9.4. Tais atvejais, kai prašymą išbraukti iš sutelktinio finansavimo platformų operatorių sąrašo pateikia pati Bendrovė, ji turi būti sudariusi susitarimą su kita sutelktinio finansavimo platforma dėl finansavimo sandorių administravimo perdavimo.

9.5. Bendrovė siekia užtikrinti, kad Bendrovės platformos administravimas būtų sklandžiai perduodamas kitam subjektui, t.y. kad neatsirastų Bendrovės platformos veiklos sutrikimų.

9.6. Bendrovės išbraukimo iš viešojo sutelktinio finansavimo operatorių sąrašo atveju už tinkamą Bendrovės įsipareigojimų vykdymą yra atsakingas Vadovas ar jo įgaliotas asmuo.

10. PROCEDŪRA, VYKDOMA BENDROVĖS NEMOKUMO ATVEJU (ĮSKAITANT RESTRUKTŪRIZAVIMO ATVEJUS)

10.1. 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.

10.2. Bendrovės nemokumo atveju:

10.2.1. nedelsiant stabdoma naujų Investuotojų registracija, naujų paskolų išmokėjimas ir Projektų savininkų paraiškų priėmimas, Finansavimo sandorių sudarymas;

10.2.2. Vadovas bendradarbiauja su priežiūros institucija ir paskirtu Bendrovės administratoriumi siekiant efektyvaus Bendrovės platformos administravimo ar jo perdavimo, Projekto finansavimo atšaukimo iš Platformos.

10.3. Už tinkamą Bendrovės pareigų vykdymą bankroto ar restruktūrizavimo atveju yra atsakingas Vadovas ir/ ar administratorius.

10.4. Bendrovei bankrutuojant, 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.

11. BAIGIAMOSIOS NUOSTATOS

11.1. Šis Planas įsigalioja nuo jo patvirtinimo dienos ir gali būti panaikintas ar pakeistas tik Vadovo įsakymu.

11.2. Už tinkamą šio Plano laikymąsi yra atsakingas Vadovas ar kitas jo paskirtas asmuo.

11.3. Šis Planas yra peržiūrimas esant poreikiui, tačiau ne rečiau nei kas 2 metus.

11.4. Popierinė Plano kopija yra saugoma Bendrovės patalpose, o elektroninė – Bendrovės serveryje.

11.5. Bendrovės darbuotojai turi būti supažindinti su Planu ir jame numatytomis jų pareigomis.

11.6. 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.

11.7. Išbandžius Plano veiksmingumą, atsakingi darbuotojai parengia Valdymo plano veiksmingumo išbandymo ataskaitą.

11.8. Išbandymo metu pastebėti trūkumai šalinami remiantis operatyvumo, veiksmingumo ir ekonomiškumo principais.