



UAB SUTELKTNIO FINANSAVIMO PLATFORMOS „REVESTUS“ PINIGŲ PLOVIMO IR TERORISTŲ FINANSAVIMO PREVENCIJOS POLITIKA	JSC CROWDFUNDING PLATFORM "REVESTUS" ANTI-MONEY LAUNDERING AND COUNTER- TERRORIST FINANCING POLICY
1. BENDROSIOS NUOSTATOS 1.1. UAB sutelktinio finansavimo platformos „Revestus“ (toliau – Bendrovė) pinigų plovimo ir teroristų finansavimo prevencijos politika (toliau – Politika) yra skirta užtikrinti, kad: 1.1.1. kiekvieno Bendrovės kliento, jo atstovo tapatybė, kai ją privaloma nustatyti, būtų nustatyta laikantis Lietuvos Respublikos pinigų plovimo ir teroristų finansavimo prevencijos įstatymo, kitų galiojančių teisės aktų reikalavimų; 1.1.2. būtų užkirstas kelias galimam pinigų plovimui ir/ar teroristų finansavimui; 1.1.3. būtų tinkamai vykdoma operacijų stebėsenos procedūra; 1.1.4. Bendrovė bendradarbiautų tik su patikimais ir reputacinės bei finansinės rizikos nekeliančiais klientais; 1.1.5. Bendrovė, bendradarbiaudama su kompetentingomis institucijomis, vykdytų kitus Lietuvos Respublikoje galiojančių teisės aktų reikalavimus. 1.2. Politika parengta vadovaujantis: 1.2.1. Lietuvos Respublikos pinigų plovimo ir teroristų finansavimo prevencijos įstatymu; 1.2.2. 2017 m. rugsėjo 12 d. Finansinių nusikaltimų tyrimo tarnybos prie Lietuvos Respublikos Vidaus reikalų ministerijos direktoriaus įsakymu Nr. V-131 „dėl asmens tapatybės dokumento kopijos tvirtinimo ir pateikimo tvarkos aprašo patvirtinimo“ patvirtintu „Asmens tapatybės dokumento kopijos tvirtinimo ir pateikimo tvarkos aprašu“; 1.2.3. 2017 m. rugsėjo 4 d. Finansinių nusikaltimų tyrimo tarnybos prie Lietuvos Respublikos Vidaus reikalų ministerijos direktoriaus įsakymu Nr. V-129 „dėl piniginių operacijų, sandorių ir klientų	1. GENERAL PROVISIONS 1.1. This Anti-Money Laundering and Counter-Terrorist Financing Policy (the "Policy") of UAB Crowdfunding Platform "Revestus" (the "Company") is intended to ensure that: 1.1.1. the identity of every Company client and, where applicable, the client's representative, is established in accordance with the requirements of the Law on the Prevention of Money Laundering and Terrorist Financing of the Republic of Lithuania and other applicable legal acts; 1.1.2. potential money laundering and/or terrorist financing is prevented; 1.1.3. transaction monitoring procedures are properly implemented; 1.1.4. the Company conducts business only with reliable clients that do not pose reputational or financial risk; 1.1.5. the Company cooperates with competent authorities and complies with all other applicable legal requirements of the Republic of Lithuania. 1.2. This Policy has been prepared in accordance with: 1.2.1. the Law on the Prevention of Money Laundering and Terrorist Financing of the Republic of Lithuania; 1.2.2. the <i>Procedure for Certification and Submission of Copies of Identity Documents</i>, approved by Order No. V-131 of 12 September 2017 of the Director of the Financial Crime Investigation Service under the Ministry of the Interior of the Republic of Lithuania; 1.2.3. the <i>Rules for Maintaining Registers of Monetary Operations, Transactions and Clients</i>, approved by Order No. V-129 of 4 September 2017 of the Director of the Financial Crime

registracijos žurnalų tvarkymo taisyklių patvirtinimo“ patvirtintomis „Piniginių operacijų, sandorių ir klientų registracijos žurnalų tvarkymo taisyklėmis“; 1.2.4. 2017 m. spalio 16 d. Lietuvos Respublikos Vidaus reikalų ministro įsakymu Nr. IV-701 „dėl įtartinų piniginių operacijų ar sandorių sustabdymo ir informacijos apie įtartinas pinigines operacijas ar sandorius pateikimo Finansinių nusikaltimų tyrimo tarnybai prie Lietuvos Respublikos Vidaus reikalų ministerijos tvarkos aprašo ir informacijos apie grynųjų pinigų operacijas ir sandorius, kurių suma lygi arba viršija 15 000 eurų ar ją atitinkančią sumą užsienio valiuta, pateikimo Finansinių nusikaltimų tyrimo tarnybai prie Lietuvos Respublikos Vidaus reikalų ministerijos tvarkos aprašo patvirtinimo“ patvirtintu „Įtartinų piniginių operacijų ar sandorių sustabdymo ir informacijos apie įtartinas pinigines operacijas ar sandorius pateikimo Finansinių nusikaltimų tyrimo tarnybai prie Lietuvos Respublikos Vidaus reikalų ministerijos tvarkos aprašu“ ir „Informacijos apie grynųjų pinigų operacijas ir sandorius, kurių suma lygi arba viršija 15 000 eurų ar ją atitinkančią sumą užsienio valiuta, pateikimo Finansinių nusikaltimų tyrimo tarnybai prie Lietuvos Respublikos Vidaus reikalų ministerijos tvarkos aprašu“; 1.2.5. 2014 m. gruodžio 5 d. Finansinių nusikaltimų tyrimo tarnybos prie Lietuvos Respublikos Vidaus reikalų ministerijos direktoriaus įsakymu Nr. V240 „dėl galimo pinigų plovimo ir įtartinų piniginių operacijų ar sandorių atpažinimo kriterijų sąrašo patvirtinimo“ patvirtintu „Galimo pinigų plovimo ir įtartinų piniginių operacijų ar sandorių atpažinimo kriterijų sąrašu“. 1.2.6. 2015 m. vasario 12 d. Lietuvos banko nutarimu Nr. 03-17 „Dėl finansų rinkos dalyviams skirtų nurodymų, kuriais siekiama užkirsti kelią pinigų plovimui ir (arba) teroristų finansavimui, patvirtinimo“. 2. SĄVOKOS 2.1. Artimas pagalbininkas:	Investigation Service under the Ministry of the Interior of the Republic of Lithuania; 1.2.4. the Procedure for the Suspension of Suspicious Monetary Operations or Transactions and the Submission of Information on Suspicious Monetary Operations or Transactions to the Financial Crime Investigation Service under the Ministry of the Interior of the Republic of Lithuania, and the Procedure for the Submission of Information on Cash Operations and Transactions Equal to or Exceeding EUR 15,000 or the Equivalent Amount in Foreign Currency to the Financial Crime Investigation Service under the Ministry of the Interior of the Republic of Lithuania, approved by Order No. IV-701 of 16 October 2017 of the Minister of the Interior of the Republic of Lithuania; 1.2.5. the <i>List of Criteria for Identifying Possible Money Laundering and Suspicious Monetary Operations or Transactions</i>, approved by Order No. V-240 of 5 December 2014 of the Director of the Financial Crime Investigation Service under the Ministry of the Interior of the Republic of Lithuania; 1.2.6. Resolution No. 03-17 of 12 February 2015 of the Board of the Bank of Lithuania <i>On the Approval of Instructions for Financial Market Participants Intended to Prevent Money Laundering and/or Terrorist Financing</i>. 2. DEFINITIONS 2.1. Close Associate means:
---	--

2.1.1. fizinis asmuo, kuris su Politikos 2.14. punkte nurodytas pareigas einančiu ar ėjusi asmeniu yra to paties juridinio asmens ar juridinio asmens statuso neturinčios organizacijos dalyvis arba palaiko kitus dalykinius santykius; 2.1.2. fizinis asmuo, kuris yra vienintelis juridinio asmens ar juridinio asmens statuso neturinčios organizacijos, įsteigtos ar veikiančios <i>de facto</i> siekiant turtinės ar kitokios asmeninės naudos Politikos 2.14. punkte nurodytas pareigas einančiam ar ėjusiam asmeniui, naudos gavėjas. 2.2. Artimieji šeimos nariai – sutuoktinis, asmuo, su kuriuo registruota partnerystė (toliau – sugyventinis), tėvai, broliai, seserys, vaikai ir vaikų sutuoktiniai, vaikų sugyventiniai. 2.3. Asmuo – Lietuvos Respublikos ar užsienio valstybės fizinis arba juridinis asmuo. 2.4. Atsakingas asmuo – Bendrovės vadovo paskirtas asmuo, atsakingas už šioje Politikoje numatytų pinigų plovimo ir (ar) teroristų finansavimo prevencijos priemonių įgyvendinimą Bendrovės veikloje; 2.5. Bendrovė – UAB sutelktinio finansavimo platforma „Revestus“, juridinio asmens kodas 306658798, buveinės adresas Konstitucijos pr. 21B, LT-08105 Vilnius. 2.6. Dalykiniai santykiai – komerciniai kliento ir Bendrovės santykiai, susiję su jų profesine veikla, kuriuos numatyta tęsti tam tikrą laikotarpį. 2.7. Darbuotojas – bet kuris Bendrovės darbuotojas, tiesiogiai dirbantis su Bendrovės klientais. 2.8. FNTT – Finansinių nusikaltimų tyrimo tarnyba prie Lietuvos Respublikos Vidaus reikalų ministerijos. 2.9. Įtartina piniginė operacija ar sandoris – piniginė operacija arba sandoris, susijęs su turtu, kuris, kaip įtariama, yra tiesiogiai arba netiesiogiai gautas iš nusikalstamos veikos arba dalyvaujant tokioje veikloje ir (ar) yra, kaip įtariama, susijęs su	2.1.1. a natural person who is a shareholder, member or participant of the same legal entity or organisation without legal personality as a person holding or having held the position referred to in Clause 2.14 of this Policy, or who maintains other close business relationships with such person; 2.1.2. a natural person who is the sole beneficial owner of a legal entity or organisation without legal personality established or operating <i>de facto</i> for the benefit of a person holding or having held the position referred to in Clause 2.14 of this Policy. 2.2. Close Family Members means a spouse, a registered partner (cohabiting partner), parents, brothers, sisters, children, spouses of children and cohabiting partners of children. 2.3. Person means a natural or legal person of the Republic of Lithuania or of a foreign state. 2.4. Responsible Person means a person appointed by the Company's Managing Director who is responsible for implementing the anti-money laundering and counter-terrorist financing measures provided for in this Policy. 2.5. Company means UAB Crowdfunding Platform "Revestus", legal entity code 306658798, registered office at Konstitucijos pr. 21B, LT-08105 Vilnius, Lithuania. 2.6. Business Relationship means a commercial relationship between the Client and the Company connected with their professional activities and intended, at the time of establishment, to have an element of duration. 2.7. Employee means any employee of the Company who works directly with the Company's clients. 2.8. FCIS means the Financial Crime Investigation Service under the Ministry of the Interior of the Republic of Lithuania. 2.9. Suspicious Monetary Operation or Transaction means a monetary operation or transaction involving property that is suspected to have been obtained, directly or indirectly, from criminal activity or participation therein and/or is
---	--

teroristų finansavimu. 2.10. Klientas – fizinis arba juridinis asmuo, kuris naudojasi Bendrovės per jos administruojamą sutelktinio finansavimo platformą „Revestus“ teikiamomis paslaugomis. 2.11. Naudos gavėjas – fizinis asmuo, kuris yra kliento (juridinio asmens ar užsienio valstybės įmonės) savininkas arba kontroliuoja klientą, ir (arba) fizinis asmuo, kurio vardu yra vykdomas sandoris ar veikla. Naudos gavėju laikomas: 2.11.1. juridiniame asmenyje: 2.11.1.1. fizinis asmuo, kuriam priklauso juridinis asmuo ar kuris jį valdo tiesiogiai ar netiesiogiai, turėdamas pakankamą procentinę dalį to juridinio asmens akcijų arba balsavimo teisių, įskaitant valdymą per pareikštines akcijas, išskyrus akcines bendroves ar kolektyvinio investavimo subjektus, kurių vertybiniais popieriais prekiaujama reguliuojamose rinkose, kuriose taikomi Europos Sąjungos teisės aktus atitinkantys reikalavimai atskleisti informaciją apie savo veiklą, arba lygiaverčiai tarptautiniai standartai, arba jį kontroliuojamas kitais būdais. Fizinis asmuo, kuris turi 25 procentus ir vieną akciją arba didesnę negu 25 procentų kliento nuosavybės dalį, yra laikomas tiesioginiu savininku. Fizinis (fiziniai) asmuo (asmens), kontroliuojantis (kontroliuojantys) įmonę arba kelias įmones, kuri (kurios) turi 25 procentus ir vieną akciją arba didesnę kaip 25 procentų kliento nuosavybės dalį, yra laikomas (laikomi) netiesioginiu (netiesioginiais) savininku (savininkais); 2.11.1.2. vyresniojo vadovo pareigas einantis fizinis asmuo, jeigu šio punkto a papunktyje nurodytas asmuo nenustatytas arba jeigu kyla abejonių, kad nustatytas asmuo yra naudos gavėjas; 2.11.2. patikos fonduose – visi šie asmenys: 2.11.2.1. patikėtojas (patikėtojai); 2.11.2.2. patikėtinis (patikėtiniai); 2.11.2.3. saugotojas (saugotojai), jeigu tokių esama;	suspected to be related to terrorist financing. 2.10. Client means a natural or legal person who uses the services provided by the Company through the crowdfunding platform Revestus administered by the Company. 2.11. Beneficial Owner means a natural person who ultimately owns or controls the Client (a legal entity or a foreign undertaking) and/or the natural person on whose behalf a transaction or activity is conducted. A Beneficial Owner shall include: 2.11.1. In the case of a legal entity: 2.11.1.1. a natural person who ultimately owns or controls the legal entity, directly or indirectly, by holding a sufficient percentage of the shares or voting rights in that legal entity, including through bearer shares, except for companies listed on regulated markets that are subject to disclosure requirements consistent with European Union legislation or equivalent international standards, or who exercises control by other means. A natural person holding 25% plus one share or an ownership interest of more than 25% in the Client shall be deemed a direct owner. A natural person (or persons) controlling one or more companies that hold 25% plus one share or an ownership interest of more than 25% in the Client shall be deemed an indirect owner. 2.11.1.2. a natural person holding the position of senior managing official, where no person referred to in Clause 2.11.1.1 has been identified or where there are doubts that the identified person is the Beneficial Owner. 2.11.2. In the case of trusts: 2.11.2.1. the settlor(s); 2.11.2.2. the trustee(s); 2.11.2.3. the protector(s), where applicable;
---	--

2.11.2.4. fiziniai asmenys, gaunantys naudą iš juridinio asmens ar juridinio asmens statuso neturinčio subjekto, arba, jeigu šie asmenys dar nenustatyti, asmenys, kurių interesams atstovauti tas juridinis asmuo ar juridinio asmens statuso neturintis subjektas yra įsteigti arba veikia; 2.11.2.5. bet koks kitas fizinis asmuo, faktiškai kontroliuojantis patikos fondą turima tiesiogine arba netiesiogine nuosavybes arba kitomis priemonėmis; 2.11.3. administruojančiame ir lėšas skirstančiame juridiniame asmenyje, į patiką panašios formos subjekte – fizinis asmuo, einantis Politikos 2.1.11.2 punkte nurodytoms pareigoms lygiavertės pareigas. 2.12. Piniginė operacija – bet koks pinigų mokėjimas, perdavimas ar gavimas. 2.13. Pinigų plovimas: 2.13.1. turto teisinės padėties pakeitimas arba turto perdavimas, žinant, kad šis turtas yra gautas iš nusikalstamos veikos arba dalyvaujant tokioje veikoje, siekiant nuslėpti arba užmaskuoti neteisėtą turto kilmę arba siekiant padėti bet kokiam nusikalstamoje veikoje dalyvaujančiam asmeniui išvengti teisinių šios veikos pasekmių; 2.13.2. turto tikrojo pobūdžio, tikrosios kilmės, šaltinio, vietos, disponavimo, judėjimo, nuosavybės teisių arba su nuosavybe susijusių teisių nuslėpimas arba užmaskavimas, žinant, kad šis turtas yra gautas iš nusikalstamos veikos arba dalyvaujant tokioje veikoje; 2.13.3. turto įgijimas, valdymas ar naudojimas, įgijimo (perdavimo) metu žinant, kad šis turtas gautas iš nusikalstamos veikos arba dalyvaujant tokioje veikoje; 2.13.4. rengimasis, pasikėsinimas padaryti, bendrininkavimas darant bet kurių iš šio punkto 1–3 papunkčiuose nurodytų veikų. 2.14. Politiškai pažeidžiami (paveikiami) asmenys (PEP) – fiziniai asmenys, kuriems yra (arba per pastaruosius 12 mėnesių buvo) patikėtos svarbios viešosios pareigos, ir jų Artimieji šeimos nariai arba Artimi pagalbininkai.	2.11.2.4. the natural persons who are beneficiaries of the legal entity or legal arrangement, or, where such persons have not yet been determined, the class of persons in whose main interest the legal entity or legal arrangement has been established or operates; 2.11.2.5. any other natural person exercising ultimate control over the trust through direct or indirect ownership or by other means. 2.11.3. In the case of a legal entity administering and distributing funds, or a legal arrangement similar to a trust, the natural person holding a position equivalent to those referred to in Clause 2.11.2 of this Policy. 2.12. Monetary Operation means any payment, transfer or receipt of funds. 2.13. Money Laundering: 2.13.1. the conversion or transfer of property, knowing that such property is derived from criminal activity or participation in such activity, for the purpose of concealing or disguising the illicit origin of the property or of assisting any person involved in such activity to evade the legal consequences of that activity; 2.13.2. the concealment or disguise of the true nature, origin, source, location, disposition, movement, ownership of, or rights with respect to, property, knowing that such property is derived from criminal activity or participation in such activity; 2.13.3. the acquisition, possession or use of property, knowing, at the time of its receipt, that it was derived from criminal activity or participation in such activity; 2.13.4. participation in, association to commit, attempts to commit, aiding, abetting, facilitating or counselling the commission of any of the acts referred to in Clauses 2.13.1–2.13.3. 2.14. Politically Exposed Persons (PEPs) means natural persons who are or have been entrusted with prominent public functions during the preceding 12 months, as well as their Close Family Members and Close Associates.
--	--

2.15. PPTFPĮ – Lietuvos Respublikos pinigų plovimo ir teroristų finansavimo prevencijos įstatymas. 2.16. Svarbios viešosios pareigos – pareigos Lietuvos Respublikoje, Europos Sąjungoje, tarptautinėse ar užsienio valstybių institucijose: 2.16.1. valstybės vadovas, vyriausybės vadovas, ministras, viceministras arba ministro pavaduotojas, valstybės sekretorius, parlamento, vyriausybės arba ministerijos kancleris; 2.16.2. parlamento narys; 2.16.3. Aukščiausiųjų Teismų, Konstitucinių Teismų ar kitų aukščiausiųjų teisminių institucijų, kurių sprendimai negali būti skundžiami, narys; 2.16.4. savivaldybės meras, savivaldybės administracijos direktorius; 2.16.5. aukščiausiosios valstybių audito ir kontrolės institucijos valdymo organo narys ar centrinio banko valdybos pirmininkas, jo pavaduotojas ar valdybos narys; 2.16.6. ambasadorius, laikinasis reikalų patikėtinis Lietuvos kariuomenės vadas, kariuomenės pajėgų ir junginių vadai, Gynybos štabo viršininkas ar užsienio valstybių aukšto rango ginkluotųjų pajėgų karininkas; 2.16.7. valstybės įmonės, akcinės bendrovės, uždarnosios akcinės bendrovės, kurių akcijos ar dalis akcijų, suteikiančių daugiau kaip 1/2 visų balsų šių bendrovių visuotiniame akcininkų susirinkime, priklauso valstybei nuosavybės teise, valdymo ar priežiūros organo narys; 2.16.8. savivaldybės įmonės, akcinės bendrovės, uždarnosios akcinės bendrovės, kurių akcijos ar dalis akcijų, suteikiančių daugiau kaip 1/2 visų balsų šių bendrovių visuotiniame akcininkų susirinkime, priklauso savivaldybei nuosavybės teise ir kurios laikomos didelėmis įmonėmis pagal Lietuvos Respublikos įmonių finansinės atskaitomybės įstatymą, valdymo ar priežiūros organo narys; 2.16.9. tarptautinės tarpyvyriausybės organizacijos vadovas, jo pavaduotojas, valdymo	2.15. AML/CFT Law means the Law on the Prevention of Money Laundering and Terrorist Financing of the Republic of Lithuania. 2.16. Prominent public functions are functions held in the Republic of Lithuania, the European Union, international organisations or foreign states, including: 2.16.1. Head of State, Head of Government, Minister, Deputy Minister or Vice-Minister, State Secretary, Chancellor of Parliament, Government or Ministry; 2.16.2. Member of Parliament; 2.16.3. Member of a Supreme Court, Constitutional Court or other high-level judicial body whose decisions are not subject to further appeal; 2.16.4. Mayor of a municipality or Director of a Municipal Administration; 2.16.5. Member of the governing body of a supreme audit or control institution or Chairperson, Deputy Chairperson or Member of the Board of a central bank; 2.16.6. Ambassador, Chargé d’Affaires, Commander of the Lithuanian Armed Forces, commanders of military forces and formations, Chief of Defence Staff, or a senior officer of the armed forces of a foreign state; 2.16.7. Member of the management or supervisory body of a state-owned enterprise, public limited company or private limited company in which the State owns shares carrying more than one-half of all voting rights at the general meeting of shareholders; 2.16.8. Member of the management or supervisory body of a municipal enterprise, public limited company or private limited company in which a municipality owns shares carrying more than one-half of all voting rights at the general meeting of shareholders and which qualifies as a large undertaking under the Law on Financial Reporting of Undertakings of the Republic of Lithuania; 2.16.9. Head, deputy head or member of the management or supervisory body of an
--	--

ar priežiūros organo narys; 2.16.10. politinės partijos vadovas, jo pavaduotojas, valdymo organo narys. 2.17. Teroristų finansavimas – veika, kuri laikoma nusikaltimu pagal 1999 m. gruodžio 9 d. Tarptautinės konvencijos dėl kovos su terorizmo finansavimu 2 straipsnį; 2.18. Trečioji šalis – kompetentingų institucijų prižiūrima finansų įstaiga, kitas įpareigotasis subjektas arba Valstybėje narėje ar Trečiojoje valstybėje registruota finansų įstaiga ar kitas įpareigotasis subjektas, atitinkantys šiuos reikalavimus: 2.18.1. jiems yra taikomas įstatymų nustatytas privalomas profesinis registravimas; 2.18.2. jie registruoti Valstybėje narėje arba Trečiojoje valstybėje, kuri taiko Europos Sąjungos nustatytiems klientų ir naudos gavėjų tapatybės nustatymo reikalavimams ir informacijos saugojimo reikalavimams lygiaverčius reikalavimus, ir kompetentingų institucijų prižiūrimi dėl šių reikalavimų laikymosi. 2.19. Trečioji valstybė – valstybė, kuri nėra Valstybė narė. 2.20. Valstybė narė – valstybė, kuri yra Europos Sąjungos arba Europos Ekonominės Erdvės valstybė narė; 2.21. Vyresnysis vadovas – pakankamai aukštas pareigas einantis pareigūnas arba darbuotojas, turintis pakankamai žinių apie įstaigai ar įmonei kylančią pinigų plovimo ir (ar) teroristų finansavimo riziką ir atsakingas už sprendimų, galinčių paveikti kylančią riziką, priėmimą. 2.22. Kitos, šiame Politikos skyriuje neapibrėžtos sąvokos suprantamos taip, kaip jos apibrėžtos PPTFPJ. 3. KLIENTO IR NAUDOS GAVĖJO TAPATYBĖS NUSTATYMAS 3.1. Bendrovė privalo imtis priemonių ir nustatyti kliento ir naudos gavėjo tapatybę šiais atvejais:	international intergovernmental organisation; 2.16.10. Leader, deputy leader or member of the governing body of a political party. 2.17. Terrorist Financing means conduct constituting an offence under Article 2 of the International Convention for the Suppression of the Financing of Terrorism of 9 December 1999. 2.18. A Third Party means a financial institution supervised by competent authorities, another obliged entity, or a financial institution or other obliged entity established in a Member State or a third country that satisfies all of the following requirements: 2.18.1. it is subject to mandatory professional registration established by law; 2.18.2. it is established in a Member State or in a third country applying customer and beneficial owner identification requirements and record-keeping requirements equivalent to those established by the European Union and is supervised by competent authorities for compliance with those requirements. 2.19. Third Country means a state that is not a Member State. 2.20. Member State means a Member State of the European Union or the European Economic Area. 2.21. Senior Manager means an officer or employee holding a sufficiently senior position, possessing adequate knowledge of the money laundering and/or terrorist financing risks faced by the institution or undertaking, and responsible for taking decisions capable of affecting those risks. 2.22. Any terms not defined in this Section of the Policy shall have the meanings assigned to them in the Law on the Prevention of Money Laundering and Terrorist Financing of the Republic of Lithuania. 3. IDENTIFICATION OF THE CUSTOMER AND THE BENEFICIAL OWNER 3.1. The Company shall take appropriate measures to identify the Customer and the
---	--

3.1.1. prieš pradėdama dalykinius santykius; 3.1.2. kai kyla abejonių dėl anksčiau gautų kliento ir naudos gavėjo tapatybės duomenų teisingumo ar autentiškumo; 3.1.3. bet kuriuo kitu atveju, kai kyla įtarimų, kad yra, buvo ar bus vykdoma pinigų plovimo ir (ar) teroristų finansavimo veika. 3.2. Bendrovės darbuotojas privalo pateikti klientui, jei klientas juridinis asmuo, kliento direktoriui, ar kliento įgaliotam atstovui užpildyti kliento anketą (anketa gali būti perkelta į paraišką projektui finansuoti), kurioje yra prašoma pateikti informaciją, reikalingą kliento ir naudos gavėjo tapatybei nustatyti. Klientui ar jo atstovui užpildžius anketą, Darbuotojas patikrina ar visi anketos laukai užpildyti. Jei yra neužpildytų laukų arba atsakymai tam tikruose laukuose yra neaiškūs, abstraktūs, Darbuotojas turi paprašyti užpildyti arba patikslinti nurodytą informaciją. Kliento užpildyta anketa naudojama kliento bei naudos gavėjo tapatybės nustatymo ir kliento bei naudos gavėjo keliamos rizikos vertinimo procese. Anketos pateikimo klientui užpildyti tikslas – surinkti kuo daugiau informacijos apie klientą, jo verslo partnerius, turto ir piniginių lėšų kilmę, vystomus verslo santykius ir jų apimtį. 3.3. Visais atvejais, kai Bendrovei kyla įtarimų, kad klientas veikia ne savo vardu, Darbuotojas turi imtis visų atitinkamų, kryptingų ir proporcingų priemonių, kad nustatytų, ar klientas veikia savo vardu, ar yra kontroliuojamas, ir nustatyti naudos gavėją, taip pat, jeigu klientas veikia per atstovą, – ir kliento atstovo tapatybę. Šiam tikslui Darbuotojas privalo užduoti klausimus ne tik tiesiogiai apie naudos gavėjus, akcininkus, tačiau	Beneficial Owner in the following cases: 3.1.1. before establishing a business relationship; 3.1.2. where there are doubts as to the accuracy or authenticity of previously obtained identification data relating to the Customer or the Beneficial Owner; 3.1.3. in any other case where there are suspicions that money laundering and/or terrorist financing has been, is being or will be carried out. 3.2. The Company's employee shall provide the Customer, or, where the Customer is a legal entity, the Customer's director or authorised representative, with a Customer Questionnaire (which may be incorporated into the project financing application), requesting the information necessary to identify the Customer and the Beneficial Owner. Upon completion of the questionnaire by the Customer or its representative, the Employee shall verify that all fields have been completed. If any fields are left incomplete or the information provided is unclear or insufficiently specific, the Employee shall request the Customer to complete or clarify the relevant information. The completed questionnaire shall be used for the purposes of Customer and Beneficial Owner identification and the assessment of the money laundering and terrorist financing risk associated with the Customer and the Beneficial Owner. The purpose of providing the questionnaire is to obtain as much information as possible regarding the Customer, its business partners, the origin of assets and funds, existing business relationships and the scope thereof. 3.3. Whenever the Company suspects that a Customer is not acting on its own behalf, the Employee shall take all appropriate, targeted and proportionate measures to determine whether the Customer is acting on its own behalf or is acting under the control of another person, identify the Beneficial Owner and, where the Customer acts through a representative, identify the representative as well. For this purpose, the
---	---

užduoti klausimus apie verslo modelį, jo funkcionavimą, ateities planus, planuojamas investicijas. Darbuotojas, pastebėjęs, kad asmuo, su kuriuo bendraujama, nežino atsakymų į dalį klausimų, susijusių su sutarties sudarymu, jos sudarymui reikalinga pateikti informacija, arba jam nepakanka žinių pagrįsti teikiamais atsakymams, apie tai turi informuoti Bendrovės direktorių ir imtis su direktoriumi suderintų veiksmų papildomam naudos gavėjo nustatymui. 3.4. Darbuotojas kliento ir naudos gavėjo tapatybės nustatymo metu turi imtis pagrįstų priemonių, kad suprastų kliento, kuris yra juridinis asmuo, nuosavybės, kontrolės struktūrą ir veiklos pobūdį, taip pat gauti informaciją apie kliento dalykinių santykių tikslą ir numatomą pobūdį, patikrinti kliento ir naudos gavėjo tapatybę. 3.5. Visais atvejais, kai yra nustatoma kliento ir naudos gavėjo tapatybės, Bendrovės darbuotojas privalo tikrinti kliento ir naudos gavėjo tapatybes, remdamasis dokumentais, duomenimis ar informacija, gauta iš patikimo ir nepriklausomo šaltinio. Darbuotojas privalo vykdyti nuolatinę kliento dalykinių santykių stebėseną. Siekiant užtikrinti, kad kliento ir naudos gavėjo tapatybės nustatymo metu pateikti dokumentai, duomenys ar informacija yra tinkami ir aktualūs, jie privalo būti nuolat peržiūrimi ir atnaujinami. 3.6. Darbuotojams draudžiama užmegzti dalykinius santykius, kai jie neturi galimybių įvykdyti šiame punkte nustatytų reikalavimų: 3.6.1. jeigu klientas nepateikia duomenų, patvirtinančių savo tapatybę, jeigu pateikia ne visus duomenis arba jie yra neteisingi, jeigu klientas ar jo atstovas vengia pateikti informaciją,	Employee shall ask questions not only concerning the Beneficial Owner and shareholders but also regarding the Customer's business model, its operation, future business plans and intended investments. If the Employee determines that the person with whom they are communicating is unable to answer questions relating to the conclusion of the agreement or the information required for entering into the agreement, or lacks sufficient knowledge to substantiate the answers provided, the Employee shall immediately inform the Company's Director and take any additional measures agreed with the Director to identify the Beneficial Owner. 3.4. During the Customer and Beneficial Owner identification process, the Employee shall take reasonable measures to understand the ownership and control structure, as well as the nature of the business activities, of Customers that are legal entities. The Employee shall also obtain information regarding the purpose and intended nature of the business relationship and verify the identity of both the Customer and the Beneficial Owner. 3.5. Whenever Customer and Beneficial Owner identification is required, the Company's Employee shall verify their identities using documents, data or information obtained from reliable and independent sources. The Employee shall also conduct ongoing monitoring of the Customer's business relationship. In order to ensure that the documents, data and information obtained during the identification process remain appropriate and up to date, they shall be reviewed and updated on a continuous basis. 3.6. Employees are prohibited from establishing business relationships where they are unable to comply with the requirements set out in this Section, including where: 3.6.1. the Customer fails to provide information confirming its identity, provides incomplete or inaccurate information, the Customer or its representative refuses or avoids providing the
--	---

reikalingą jo tapatybei nustatyti, slepia naudos gavėjo tapatybę ar vengia pateikti informaciją, reikalingą naudos gavėjo tapatybei nustatyti, arba pateiktų duomenų tam neužtenka; 3.6.2. jeigu Bendrovė negali užtikrinti tinkamo Politikos 3.3. – 3.5. papunkčių reikalavimų vykdymo. Apie tokius atvejus, įvertinus keliamą pinigų plovimo ir teroristų finansavimo grėsmę, Darbuotojas privalo nedelsiant pranešti Bendrovės direktoriui, o direktorius, esant pagrindui, ir FNTT; 3.6.3. Dalykinius santykius taip pat draudžiama užmegzti, jei patikrinus klientą nustatoma, kad klientas yra susijęs su asmenimis, jų grupėmis bei įmonėmis ir įstaigomis, kurioms taikomos Jungtinių Tautų, Europos Sąjungos bei kitų tarptautinių organizacijų nustatytos sankcijos. Patikras galima atlikti Lietuvos Respublikos užsienio reikalų ministerijos interneto puslapyje (https://www.urm.lt/sankcijos). 3.7. Jeigu klientas vengia arba atsisako Darbuotojui jo prašymu ir terminais pateikti informaciją apie piniginių lėšų ar turto kilmę, kitus papildomus duomenis, Bendrovės Darbuotojas gali inicijuoti dalykinių santykių su klientu iki prašomos informacijos pateikimo sustabdymą arba dalykinių santykių su klientu nutraukimą, informuodamas apie šias aplinkybes direktorių. Sprendimą dėl dalykinių santykių su klientu sustabdymo arba nutraukimo priima direktorius. Kai klientas piktybiškai neteikia prašomos informacijos, vengia pateikti informaciją apie lėšų ir turto kilmę arba teikia melagingą informaciją, direktorius priima sprendimą nutraukti dalykinius santykius su klientu. 3.8. Darbuotojas nedelsdamas turi iš naujo nustatyti kliento tapatybę, taikydamas sustiprintą kliento tapatybės nustatymą, šiais atvejais: 3.8.1. kai klientas savo tapatybei nustatyti pateikia informaciją, žinodamas, kad ji neteisinga; 3.8.2. kai klientas nuslepia informaciją;	information required for identification, conceals the identity of the Beneficial Owner or refuses to provide information necessary for identifying the Beneficial Owner, or where the information provided is insufficient for such identification; 3.6.2. the Company is unable to ensure proper compliance with the requirements set out in Clauses 3.3–3.5 of this Policy. In such cases, having assessed the money laundering and terrorist financing risk, the Employee shall immediately inform the Company's Director and, where appropriate, the Director shall notify the Financial Crime Investigation Service (FCIS); 3.6.3. business relationships shall also not be established where the Customer is found to be associated with persons, groups, companies or institutions subject to sanctions imposed by the United Nations, the European Union or other international organisations. Such checks may be performed using the sanctions database published by the Ministry of Foreign Affairs of the Republic of Lithuania. 3.7. Where the Customer refuses or fails to provide information regarding the origin of funds or assets, or any other additional information requested by the Employee within the specified deadline, the Employee may initiate the suspension of the business relationship until the requested information is provided or propose the termination of the business relationship, informing the Company's Director accordingly. The decision on suspension or termination shall be made by the Director. Where the Customer deliberately refuses to provide the requested information, conceals the origin of funds or assets or provides false information, the Director shall terminate the business relationship. 3.8. The Employee shall immediately repeat the Customer identification process by applying Enhanced Customer Due Diligence in the following cases: 3.8.1. where the Customer knowingly provides false information for identification purposes; 3.8.2. where the Customer conceals relevant
---	---

3.8.3. kai atsiranda aplinkybės Politikos 7.2. punkte numatytais atvejais taikyti sustiprintą tapatybės nustatymą. 3.9. Paaiškėjus, kad klientas savo ar naudos gavėjo tapatybei nustatyti pateikė informaciją, žinodamas, kad ji neteisinga, arba kai klientas nuslepia informaciją, Darbuotojas turi išsiaiškinti dėl kokių priežasčių buvo pateikta neteisinga informacija ir apie šias aplinkybes nedelsdamas informuoti Bendrovės direktorių. Bendrovės direktorius turi ne vėliau kaip per 2 (dvi) darbo dienas išanalizuoti pateiktą informaciją ir nustatęs, kad kliento veiksmuose galimai buvo bandymų nuslėpti tam tikrą informaciją, siekiant atlikti neteisėtus veiksmus, informuoti apie šį klientą ir jo veiksmus FNTT. 3.10. Informacija apie klientus, kurių tapatybė nustatoma vadovaujantis Politikos 7 skyriaus nuostatomis, ir šių klientų naudos gavėjus turi būti atnaujinama ne rečiau kaip kas 2 (dvejus) metus. 3.11. Nustačius, kad naudos gavėjas yra kitas nei Politikos 3.9. punkte nurodytas fizinis asmuo, Darbuotojas apie tai privalo informuoti direktorių. Su tokiais klientais dalykiniai santykiai pradedami tik gavus direktoriaus pritarimą. 3.12. Bendrovė nėra atsakinga klientui už sutartinių įsipareigojimų nevykdymą ir žalą, padarytą dėl kliento piniginių operacijų ar sandorių nevykdymo, jeigu Bendrovė kliento piniginių operacijų ar sandorių nevykdė dėl šioje Politikoje nurodytų priežasčių. 4. KLIENTO TAPATYBĖS NUSTATYMAS KLIENTUI DALYVAUJANT FIZIŠKAI 4.1. Darbuotojai, kai kliento tapatybė nustatoma jam dalyvaujant fiziškai, reikalauja iš kliento – fizinio asmens Lietuvos Respublikos ar užsienio valstybės asmens tapatybės dokumento arba leidimo gyventi Lietuvos Respublikoje, arba 2006	information; 3.8.3. where circumstances arise requiring the application of enhanced due diligence under Clause 7.2 of this Policy. 3.9. Where it becomes apparent that the Customer has knowingly provided false information for the purposes of identifying itself or the Beneficial Owner, or has concealed relevant information, the Employee shall establish the reasons for such conduct and immediately inform the Company's Director. Within 2 (two) business days, the Director shall assess the information received and, where it appears that the Customer has attempted to conceal information in order to facilitate unlawful activities, the Director shall report the Customer and the relevant circumstances to the Financial Crime Investigation Service (FCIS). 3.10. Information relating to Customers whose identification is carried out in accordance with Section 7 of this Policy, and their Beneficial Owners, shall be updated at least once every 2 (two) years. 3.11. Where it is established that the Beneficial Owner is a person other than the natural person referred to in Clause 3.9 of this Policy, the Employee shall immediately inform the Company's Director. Business relationships with such Customers may only be established upon the Director's approval. 3.12. The Company shall not be liable to the Customer for any failure to perform contractual obligations or for any losses resulting from the Company's refusal to execute the Customer's transactions where such refusal is based on the grounds set out in this Policy. 4. CUSTOMER IDENTIFICATION IN THE CUSTOMER'S PHYSICAL PRESENCE 4.1. Where the Customer's identity is established in the Customer's physical presence, the Employee shall require the Customer, if the Customer is a natural person, to present a passport or national identity card issued by the
--	---

m. gruodžio 20 d. Europos Parlamento ir Tarybos direktyvos 2006/126/EB dėl vairuotojo pažymėjimų (nauja redakcija) I priede nustatytus reikalavimus atitinkančio Europos ekonominės erdvės valstybėje išduoto vairuotojo pažymėjimo, kuriame yra šie duomenys, patvirtinantys jo tapatybę (toliau vadinama – tapatybę patvirtinantis dokumentas): vardas (vardai), pavardė (pavardės), asmens kodas (užsieniečiui – gimimo data (jeigu yra – asmens kodas ar kita šiam asmeniui suteikta unikali simbolių seka, skirta asmeniui identifikuoti), leidimo gyventi Lietuvos Respublikoje numeris ir galiojimo laikas, jo išdavimo vieta ir data (taikoma užsieniečiams), nuotrauka, parašas (išskyrus atvejus, kai tapatybę patvirtinančiame dokumente jis neprivalomas), pilietybė (išskyrus atvejus, kai tapatybę patvirtinančiame dokumente ji neprivaloma), jeigu asmuo be pilietybės, – valstybė, kuri išdavė asmens tapatybę patvirtinantį dokumentą. Kai tapatybę patvirtinančiame dokumente duomenys apie kliento pilietybę nenurodomi, Bendrovės darbuotojas nustatydamas kliento – fizinio asmens tapatybę, kai ji nustatoma jam dalyvaujant fiziškai, privalo pareikalauti iš kliento duomenų apie pilietybę.

4.2. Kai klientas yra juridinis asmuo, atstovaujamas fizinio asmens, arba klientui – fiziniam asmeniui atstovauja kitas fizinis asmuo, šių atstovų tapatybė nustatoma taip pat, kaip ir kliento – fizinio asmens. Taip pat klientas turi pateikti informaciją apie juridinio asmens vadovą: vadovo vardas, pavardė, asmens kodas (užsieniečiui – gimimo data (jeigu yra, – asmens kodas ar kita šiam asmeniui suteikta unikali simbolių seka, skirta asmeniui identifikuoti), pilietybė (jeigu asmuo be pilietybės, – valstybė, kuri išdavė asmens tapatybę patvirtinantį dokumentą).

4.3. Darbuotojai, reikalauja iš kliento – juridinio asmens jo tapatybę patvirtinančių dokumentų arba šių dokumentų kopijų su notaro liudijimu, patvirtinančiu dokumento kopijos tikrumą,

Republic of Lithuania or a foreign state, a residence permit issued by the Republic of Lithuania, or a driving licence issued by a Member State of the European Economic Area that complies with the requirements set out in Annex I to Directive 2006/126/EC of the European Parliament and of the Council of 20 December 2006 on driving licences (recast), containing the following identification data (hereinafter – Identity Document): first name(s); surname(s); personal identification number (or, for foreign nationals, date of birth and, where applicable, personal identification number or another unique personal identifier); number of the residence permit in the Republic of Lithuania, its date and place of issue and validity period (where applicable to foreign nationals); photograph; signature (except where not required by the Identity Document); nationality (except where not required by the Identity Document); and where the person is stateless, the state that issued the Identity Document. Where the Customer's nationality is not indicated in the Identity Document, the Employee shall require the Customer to provide information regarding their nationality.

4.2. Where the Customer is a legal entity represented by a natural person, or where a natural person is represented by another natural person, the representative's identity shall be established in the same manner as that of a natural person. In addition, information regarding the legal entity's director shall be obtained, including: first name; surname; personal identification number (or, for foreign nationals, date of birth and, where applicable, personal identification number or another unique personal identifier); nationality (or, where the person is stateless, the state that issued the Identity Document).

4.3. The Employee shall require a legal entity Customer to provide documents (or notarised copies thereof) confirming its identity and containing at least the following information:

kuriuose yra šie duomenys: pavadinimas, teisinė forma, buveinė, faktinės veiklos vykdymo adresas, kodas (jei toks yra suteiktas), Juridinių asmenų registro išrašas ir jo išdavimo data, juridinio asmens vardu pagal įgaliojimą veikiančių atstovų duomenys, nurodyti Politikos 4.2. punkte, juridinio asmens veiklos rūšys, dalykinių santykių tikslai, objektas ir ūkinės komercinės veiklos pobūdis. 4.4. Bendrovė turi teisę gauti Politikos 4.1. – 4.3. punktuose nurodytus kliento ir naudos gavėjo tapatybei nustatyti reikalingus dokumentus, duomenis ar informaciją tiesiogiai iš Lietuvos Respublikos ir (ar) kitų valstybių informacinių sistemų ar registrų, o tais atvejais, kai Europos Sąjungos valstybėje narėje atitinkami dokumentai, duomenys ar informacija nėra kaupiami valstybės informacinėse sistemose ar registruose, – ir iš kitų patikimų ir nepriklausomų duomenų bazių ar registrų ir nereikalauti iš kliento, kad jis pats pateiktų šiuos dokumentus, duomenis ar informaciją, jeigu klientas Bendrovės dokumentus, duomenis ar informaciją, gautus tiesiogiai iš valstybės informacinių sistemų ar registrų arba kitų patikimų ir nepriklausomų duomenų bazių ar registrų, patvirtina parašu (įskaitant kvalifikuotą elektroninį parašą). Bendrovės darbuotojas gali nereikalauti, kad klientas Bendrovės tiesiogiai iš Lietuvos Respublikos ir (ar) kitų valstybių informacinių sistemų ar registrų gautus dokumentus, duomenis ar informaciją patvirtintų parašu, jeigu tokie dokumentai, duomenys ar informacija nesiskiria nuo anksčiau kliento parašu patvirtintų dokumentų, duomenų ar informacijos, taip pat jeigu tokie dokumentai, duomenys ar informacija gauti iš Lietuvos Respublikos ir (ar) kitų Europos Sąjungos valstybių narių informacinių sistemų ir (ar) registrų, o tais atvejais, kai Europos Sąjungos valstybėje narėje atitinkami dokumentai, duomenys ar informacija nėra kaupiami valstybės informacinėse sistemose ar registruose, – ir iš kitų patikimų ir nepriklausomų duomenų bazių ar registrų.	name; legal form; registered office; principal place of business; registration number (if assigned); extract from the Register of Legal Entities and the date of its issue; details of authorised representatives acting on behalf of the legal entity, as specified in Clause 4.2 of this Policy; business activities; purpose of the business relationship; and nature of the commercial and economic activities. 4.4. The Company shall have the right to obtain the documents, data and information necessary for the identification of the Customer and the Beneficial Owner referred to in Clauses 4.1–4.3 directly from information systems or registers of the Republic of Lithuania and/or other states. Where the relevant information is not maintained in public registers of an EU Member State, the Company may obtain such information from other reliable and independent databases or registers and shall not require the Customer to provide such documents or information, provided that the Customer confirms, by signature (including a qualified electronic signature), the information obtained by the Company. The Employee may also waive the requirement for the Customer to confirm such information by signature where: the information does not differ from information previously confirmed by the Customer; or the information has been obtained directly from official information systems or registers of the Republic of Lithuania or another EU Member State, or, where applicable, from other reliable and independent databases or registers.
--	---

4.5. Pradėdamas kliento tapatybės nustatymą, kai klientas – fizinis asmuo arba kliento – juridinio asmens atstovas, nustatant jo tapatybę, dalyvauja fiziškai, Darbuotojas privalo: 4.5.1. įvertinti, ar klientas (arba kliento atstovas) – fizinis asmuo, pradedantis bendradarbiauti su Bendrove, pateikia galiojančius tapatybę patvirtinančius dokumentus; nustatyti, ar jo pateiktame dokumente yra būtent to kliento nuotrauka. Gavęs tapatybės dokumentą išduotą Lietuvos Respublikoje, Darbuotojas patikrina jį negaliojančių asmens dokumentų duomenų bazėje (https://www.ird.lt/lt/paslaugos/informacijos-rinkmenos/paieska-negaliojanciu-asmens-dokumentu-duomenu-bazeje). Nustatęs, kad asmens dokumentas negaliojantis, Darbuotojas privalo paprašyti pateikti galiojantį asmens dokumentą; 4.5.2. įvertinti pateikto dokumento būklę (ypač didelį dėmesį atkreipti į tai, ar nuotrauka, puslapiai ar įrašai nebuvo keičiami, taisomi, ir panašiai); 4.5.3. sužinoti, ar klientas – fizinis ar juridinis asmuo pats naudosis Bendrovės paslaugomis, ar jis atstovaus kito asmens interesams; 4.5.4. įsitikinti, ar fizinis ar juridinis asmuo turi reikiamus įgaliojimus veikti kliento vardu; 4.5.5. padaryti fizinio asmens pateikto tapatybę patvirtinančio dokumento puslapių, kuriuose yra šio fizinio asmens nuotrauka ir kiti tapatybei nustatyti reikalingi duomenys, kopiją arba nuskenuoti dokumentą; 4.5.6. kai reikia nustatyti užsieniečio kliento tapatybę, padaryti tapatybę patvirtinančio dokumento; 4.5.7. laikydamasis Politikoje nustatytos tvarkos, imtis veiksmų, pagrindžiančių būtinumą taikyti sustiprintą tapatybės nustatymą. 4.6. Jeigu klientas yra juridinis asmuo, atstovaujamas fizinio asmens, arba klientui – fiziniui asmeniui – atstovauja kitas fizinis asmuo, Darbuotojas turi pareikalauti iš jo įgaliojimo ir	4.5. When commencing the identification of a Customer who is a natural person, or of the representative of a legal entity in the Customer's physical presence, the Employee shall: 4.5.1. verify that the Customer (or representative) presents a valid Identity Document and confirm that the photograph contained therein corresponds to the person presenting it. Where the document has been issued by the Republic of Lithuania, the Employee shall verify its validity using the national database of invalid identity documents. If the document is invalid, the Employee shall require the Customer to present another valid Identity Document; 4.5.2. examine the physical condition of the document, paying particular attention to any indications that photographs, pages or entries have been altered, replaced or tampered with; 4.5.3. determine whether the Customer is acting on their own behalf or on behalf of another person; 4.5.4. verify that the representative has the necessary authority to act on behalf of the Customer; 4.5.5. make a copy or scan of the pages of the Identity Document containing the Customer's photograph and the information required for identification; 4.5.6. where the Customer is a foreign national, make a copy or scan of the relevant Identity Document; 4.5.7. assess, in accordance with this Policy, whether Enhanced Customer Due Diligence measures should be applied. 4.6. Where a legal entity Customer is represented by a natural person, or a natural person is represented by another natural person, the Employee shall require the representative to
---	--

patikrinti jo galiojimą (tai yra jį išdavusio asmens teisę išduoti tokį įgaliojimą), įgaliojimo galiojimo laiką, kokius veiksmus atlikti nurodyta įgaliojime (Lietuvos Respublikoje išduotas įgaliojimas turi atitikti Lietuvos Respublikos civilinio kodekso reikalavimus, jame būtinai turi būti nurodyta išrašymo data ir jis patvirtintas juridinio asmens antspaudu, jei juridinis asmuo privalo turėti antspaudą, užsienyje išduotas įgaliojimas turi būti legalizuotas arba patvirtintas dokumentų tvirtinimo pažyma (<i>apostille</i>)), išskyrus įgaliojimus, išduotus Europos Sąjungos valstybėse narėse. 4.7. Tapatybei nustatyti turi būti pateikti dokumentų originalai arba šių dokumentų kopijos, patvirtintos notarų, konsulinių pareigūnų. 4.8. Ant kiekvieno kliento tapatybę patvirtinančio dokumento kopijos (jeigu daroma popierinė dokumento kopija) Darbuotojas, padaręs dokumento kopiją, privalo uždėti tikrumo žymą. Tikrumo žymą sudaro žodžiai „Kopija tikra“, Darbuotojo pareigų pavadinimas, parašas, vardas ir pavardė, kopijos padarymo data, Bendrovės antspaudas. Jei popierinė dokumento kopija nėra daroma, nuskenuota dokumento kopija turi būti saugoma skaitmeninėje kliento byloje. 4.9. Jei klientui, kuris yra juridinis asmuo, atstovauja kitas juridinis arba fizinis asmuo ir tokio atstovavimo pagrindai yra nustatyti kliento steigimo dokumentuose, Bendrovės darbuotojai privalomai patikrina asmens paskyrimo į atitinkamą kliento valdymo organą dokumentą bei susipažįsta su tokiais faktais patvirtinančia kliento steigimo dokumentų (įstatų ir pan.) dalimi arba susipažįsta su išrašu iš registro, kuris patvirtina, kad asmuo turi teisę veikti kliento vardu. 4.10. Kiekvieną kartą pradedant dalykinius santykius su klientu Bendrovės darbuotojai privalomai informuoja klientą apie jo pareigą nedelsiant raštu informuoti Bendrovę apie jo atstovo įgaliojimų panaikinimą, pasibaigimą ar įgaliojimų apimties pasikeitimą. Iki tokios	provide the relevant power of attorney and verify: its validity; the authority of the person issuing it; its validity period; and the scope of the representative's authority. A power of attorney issued in the Republic of Lithuania must comply with the requirements of the Civil Code of the Republic of Lithuania, contain the date of issue and, where applicable, bear the seal of the legal entity. A power of attorney issued abroad must be legalised or certified by an apostille, unless issued in another Member State of the European Union. 4.7. Original documents or copies certified by a notary public or consular officer shall be submitted for identification purposes. 4.8. Where paper copies of identity documents are made, the Employee shall certify each copy by affixing a certification statement containing the words "Certified True Copy", together with the Employee's position, signature, full name, the date of certification and the Company's official seal. Where no paper copy is made, the scanned copy shall be stored electronically in the Customer's digital file. 4.9. Where a legal entity Customer is represented by another legal or natural person and such representation is based on the legal entity's constitutional documents, the Employee shall verify the appointment document confirming the representative's position and review the relevant provisions of the constitutional documents (such as the Articles of Association) or obtain an extract from the relevant register confirming the representative's authority to act on behalf of the Customer. 4.10. Upon establishing a business relationship, the Employee shall inform the Customer of its obligation to notify the Company immediately in writing of any revocation, expiry or amendment of the representative's authority. Until such notification is received, the Company shall be
--	---

informacijos pateikimo Bendrovei laikoma, kad atstovo įgaliojimai nėra pasibaigę, nebent Bendrovė žinojo ar turėjo žinoti apie kliento atstovo įgaliojimų panaikinimą, pasibaigimą ar įgaliojimų apimties pasikeitimą. 5. KLIENTO TAPATYBĖS NUSTATYMAS NUOTOLINIŲ BŪDU 5.1. Bendrovė gali nustatyti kliento ir naudos gavėjo tapatybę, kai kliento ir naudos gavėjo tapatybė nustatoma jam nedalyvaujant fiziškai, naudojantis elektroninėmis priemonėmis leidžiančiomis tiesioginį vaizdo perdavimą vienu iš šių būdų: 5.1.1. naudojantis Trečiųjų šalių informacija apie klientą ar naudos gavėją; 5.1.2. naudojant Europos Sąjungoje išduotas elektroninės atpažinties priemones, veikiančias pagal aukšto arba pakankamo saugumo užtikrinimo lygio elektroninės atpažinties schemas, nustatytas 2014 m. liepos 23 d. Europos Parlamento ir Tarybos reglamente (ES) Nr. 910/2014 dėl elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų vidaus rinkoje, kuriuo panaikinama Direktyva 1999/93/EB; 5.1.3. kai informacija apie asmens tapatybę tvirtinama kvalifikuotu elektroniniu parašu, naudojant kvalifikuotą elektroninio parašo sertifikatą, kuris atitinka Reglamento (ES) Nr. 910/2014 reikalavimus. Trečiųjų valstybių kvalifikuoti elektroniniai parašai, sudaryti naudojant kvalifikuotą elektroninio parašo sertifikatą, pripažįstami vadovaujantis Reglamento (ES) Nr. 910/2014 14 str.; 5.1.4. naudojant elektroninės priemones, leidžiančias tiesioginį vaizdo perdavimą vienu iš šių būdų: 5.1.4.1. tiesioginio vaizdo perdavimo metu užfiksuojamas Kliento tapatybę patvirtinančio dokumento originalas ir Kliento tapatybę patvirtinama naudojantis pažangiuoju elektroniniu parašu, atitinkančiu Reglamento (ES)	entitled to assume that the representative's authority remains valid, unless the Company knew or ought reasonably to have known that such authority had expired, been revoked or otherwise changed. 5. REMOTE CUSTOMER IDENTIFICATION 5.1. The Company may identify the Customer and the Beneficial Owner where they are not physically present by using electronic means that enable live video transmission, in any of the following ways: 5.1.1. by relying on information about the Customer or the Beneficial Owner obtained from Third Parties; 5.1.2. by using electronic identification means issued in the European Union and operating under electronic identification schemes with a high or substantial level of assurance, as provided for in Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC; 5.1.3. where identity information is confirmed by a qualified electronic signature using a qualified certificate for electronic signatures that complies with Regulation (EU) No 910/2014. Qualified electronic signatures from third countries, created using a qualified certificate for electronic signatures, shall be recognised in accordance with Article 14 of Regulation (EU) No 910/2014; 5.1.4. by using electronic means enabling live video transmission in one of the following ways: 5.1.4.1. during live video transmission, the original Identity Document of the Customer is captured and the Customer's identity is confirmed using an advanced electronic signature meeting the requirements of Article 26 of Regulation (EU) No
--	---

Nr. 910/2014 26 straipsnyje nustatytus reikalavimus; 5.1.4.2. tiesioginio vaizdo perdavimo metu užfiksuojamas Kliento veido atvaizdas ir Kliento parodytas tapatybę patvirtinančio dokumento originalas. 5.2. Nustatant kliento ir naudos gavėjo tapatybę šios Politikos 5.1.1. – 5.1.3. punktuose nurodytais atvejais, Bendrovė privalo laikytis šių sąlygų: 5.2.1. prieš nustatant kliento ir naudos gavėjo tapatybę šios Politikos 5.1.1. – 5.1.2. punktuose nurodytais atvejais kliento tapatybė Trečiosios šalies buvo nustatyta jam fiziškai dalyvaujant arba naudojant elektronines priemones, leidžiančias tiesioginį vaizdo perdavimą vienu iš būdų, nurodytų šios Politikos 5.1.4. punkte, taip pat kai kliento tapatybė buvo nustatyta jam fiziškai dalyvaujant išduodant elektroninės atpažinties priemonę, veikiančią pagal aukšto arba pakankamo saugumo užtikrinimo lygio elektroninės atpažinties schema; 5.2.2. prieš nustatant kliento ir naudos gavėjo tapatybę šios Politikos 5.1.1. – 5.1.3. punktuose nurodytais atvejais, kliento ir naudos gavėjo – fizinio asmens ir juridinio asmens atstovo tapatybė buvo nustatyta iš Politikos 4 skyriuje nurodytų dokumentų. 5.3. Nustatydami kliento ir naudos gavėjo tapatybę pagal Politikos 5 skyrių, Darbuotojai privalo imtis 4 skyriuje nustatytų priemonių ir nustatyti bei patikrinti ir kliento, ir naudos gavėjo tapatybę, kliento ir naudos gavėjo tapatybei nustatyti panaudoti papildomus duomenis, dokumentus ar papildomą informaciją, kuri leistų įsitikinti kliento tapatybės autentiškumu, patikrinti ar yra aplinkybių taikyti sustiprintą kliento tapatybės nustatymą. 5.4. Bendrovė gali pasitelkti trečiuosius asmenis ir jų siūlomus technologinius sprendimus kliento	910/2014; 5.1.4.2. during live video transmission, the Customer's facial image and the original Identity Document presented by the Customer are captured. 5.2. When identifying the Customer and the Beneficial Owner in the cases referred to in Clauses 5.1.1–5.1.3 of this Policy, the Company shall comply with the following conditions: 5.2.1. before the Customer and the Beneficial Owner are identified in the cases referred to in Clauses 5.1.1–5.1.2 of this Policy, the Customer's identity must have been established by the Third Party either in the Customer's physical presence or by using electronic means enabling live video transmission in one of the ways specified in Clause 5.1.4 of this Policy, or the Customer's identity must have been established in the Customer's physical presence when issuing an electronic identification means operating under an electronic identification scheme with a high or substantial level of assurance; 5.2.2. before the Customer and the Beneficial Owner are identified in the cases referred to in Clauses 5.1.1–5.1.3 of this Policy, the identity of the Customer, the Beneficial Owner who is a natural person, and the representative of a legal entity must have been established on the basis of the documents specified in Section 4 of this Policy. 5.3. When identifying the Customer and the Beneficial Owner in accordance with Section 5 of this Policy, Employees shall take the measures set out in Section 4 and shall identify and verify both the Customer and the Beneficial Owner. Employees shall use additional data, documents or information for the identification of the Customer and the Beneficial Owner in order to confirm the authenticity of the Customer's identity and verify whether circumstances exist requiring the application of Enhanced Customer Due Diligence. 5.4. The Company may engage third parties and use their technological solutions to identify the
---	---

tapatybei jam fiziškai nedalyvaujant nustatyti. Tokiu atveju Bendrovė užtikrina, kad visa kliento ir naudos gavėjo tapatybės nustatymo metu surinkta informacija būtų perduodama Bendrovei ir saugoma kliento byloje arba tokią informaciją pasitelkęs asmuo sutartimi būtų įsipareigojęs pateikti pagal Bendrovės prašymą. Be kita ko, kliento byloje Bendrovė saugo tiesioginio vaizdo perdavimo metu surinktą informaciją, kliento patikrinimo tarptautiniuose finansinių sankcijų sąrašuose ir politiškai pažeidžiamų asmenų sąrašuose surinktą informaciją. 5.5. Nustatydama kliento tapatybę, Bendrovė gali naudotis Trečiųjų šalių paslaugomis ir jų teikiama informacija. Prieš nustatant kliento ir naudos gavėjo tapatybę, remiantis Trečiųjų šalių informacija, Bendrovė privalo užtikrinti, kad: 5.5.1. kliento tapatybė Trečiosios šalies buvo nustatyta vienu iš šių būdų: 5.5.1.1. jam fiziškai dalyvaujant iš asmens tapatybę patvirtinančio dokumento, arba išrašo iš juridinių asmenų registro, arba juridinio asmens steigimo dokumentų; 5.5.1.2. panaudojant elektronines priemones, leidžiančias tiesioginį vaizdo perdavimą 5.5.1.3. atliekant mokėjimą į Trečiosios šalies mokėjimo sąskaitą iš Kliento vardu kredito įstaigoje, kuri yra registruota Valstybėje narėje arba Trečiojoje valstybėje, nustačiusioje įstatymo reikalavimams lygiaverčius reikalavimus, ir kompetentingų institucijų prižiūrima dėl šių reikalavimų laikymosi, turimos sąskaitos ir pateikiant Lietuvos Respublikos teisės aktų nustatyta tvarka patvirtintą popierinę asmens tapatybės dokumento kopiją; 5.5.2. Trečioji šalis, Bendrovei paprašius, nedelsdama pateiks visą prašomą informaciją ir duomenis, privalomus turėti laikantis PPTFPĮ ir Politikoje nurodytų Kliento ar Naudos gavėjo tapatybės nustatymo reikalavimų;	Customer remotely. In such case, the Company shall ensure that all information collected during the identification of the Customer and the Beneficial Owner is transferred to the Company and stored in the Customer file, or that the engaged service provider is contractually obliged to provide such information at the Company's request. In particular, the Company shall store in the Customer file information collected during live video transmission and information obtained from screening the Customer against international financial sanctions lists and politically exposed persons lists. 5.5. When identifying the Customer, the Company may use the services of Third Parties and rely on information provided by them. Before identifying the Customer and the Beneficial Owner on the basis of Third Party information, the Company shall ensure that: 5.5.1. the Third Party has identified the Customer in one of the following ways: 5.5.1.1. in the Customer's physical presence on the basis of an Identity Document, an extract from the register of legal entities or the constitutional documents of the legal entity; 5.5.1.2. by using electronic means enabling live video transmission; 5.5.1.3. by making a payment to the Third Party's payment account from an account held in the Customer's name with a credit institution established in a Member State or in a Third Country that has established requirements equivalent to those of the AML/CFT Law and is supervised by competent authorities for compliance with such requirements, together with the submission of a paper copy of the Identity Document certified in accordance with the legal acts of the Republic of Lithuania; 5.5.2. upon the Company's request, the Third Party will immediately provide all requested information and data that must be obtained in accordance with the AML/CFT Law and the Customer or Beneficial Owner identification requirements set out in this Policy;
--	--

5.5.3. Trečioji šalis, Bendrovei paprašius, nedelsdama pateiks dokumentų, susijusių su kliento ar naudos gavėjo tapatybės nustatymu, kopijas ir kitus dokumentus, susijusius su klientu ar naudos gavėju, kurie privalomi turėti laikantis PPTFPĮ ir Politikoje nurodytų kliento ar naudos gavėjo tapatybės nustatymo reikalavimų. 5.6. Pasitelkdama kliento tapatybės nustatymui Trečiąją šalį, Bendrovė neprivalo gauti kiekvieno kliento asmens dokumento ir atlikti jo patikrą. 5.7. Pasirinkdama Trečiąją šalį, kurios pateikta informacija bus vadovaujama nustatant kliento ir naudos gavėjo tapatybę, Bendrovė atsižvelgia į tai, kad atsakomybė dėl PPTFPĮ ir Politikoje kliento ar naudos gavėjo tapatybės nustatymo reikalavimų laikymosi tenka Bendrovei. 6. NAUDOS GAVĖJO TAPATYBĖS NUSTATYMAS 6.1. Nustatant kliento tapatybę, visais atvejais privaloma nustatyti naudos gavėją. Naudos gavėjo nustatymas visais atvejais reiškia fizinio asmens ar fizinių asmenų grupės nustatymą. 6.2. Darbuotojai, nustatydami naudos gavėjo tapatybę, kai kliento ir naudos gavėjo tapatybė nustatoma klientui dalyvaujant fiziškai, privalo pareikalauti iš kliento ir naudos gavėjo tapatybės duomenų: vardas (-ai), pavardė (-ės), asmens kodas (užsieniečiui – gimimo data (jeigu yra, – asmens kodas ar kita šiam asmeniui suteikta unikali simbolių seka, skirta asmeniui identifikuoti, leidimo gyventi Lietuvos Respublikoje numeris ir galiojimo laikas, jo išdavimo vieta ir data), pilietybė (jeigu asmuo be pilietybės, – valstybė, kuri išdavė asmens tapatybę patvirtinantį dokumentą). 6.3. Darbuotojai tikrina kliento pateiktus dokumentus ir informaciją apie naudos gavėją, remdamiesi dokumentais, duomenimis ar informacija, gautais iš patikimo ir nepriklausomo	5.5.3. upon the Company's request, the Third Party will immediately provide copies of documents relating to the identification of the Customer or Beneficial Owner, as well as other documents relating to the Customer or Beneficial Owner that must be obtained in accordance with the AML/CFT Law and the identification requirements set out in this Policy. 5.6. Where the Company relies on a Third Party for Customer identification, the Company is not required to obtain and verify each Customer's Identity Document itself. 5.7. When selecting a Third Party whose information will be relied upon for the identification of the Customer and the Beneficial Owner, the Company shall take into account that responsibility for compliance with the Customer and Beneficial Owner identification requirements under the AML/CFT Law and this Policy remains with the Company. 6. IDENTIFICATION OF THE BENEFICIAL OWNER 6.1. When identifying a Customer, the Beneficial Owner shall always be identified. Identification of the Beneficial Owner shall in all cases mean identifying a natural person or a group of natural persons. 6.2. When identifying the Beneficial Owner in the Customer's physical presence, Employees shall require the Customer to provide the following identification data of the Beneficial Owner: first name(s); surname(s); personal identification number or, for foreign nationals, date of birth and, where applicable, personal identification number or another unique personal identifier assigned to the person; number and validity period of the residence permit in the Republic of Lithuania, and its place and date of issue, where applicable; nationality or, where the person is stateless, the state that issued the Identity Document. 6.3. Employees shall verify the documents and information provided by the Customer regarding the Beneficial Owner using documents, data or information obtained from reliable and
--	--

šaltinio. Tokie Darbuotojo veiksmai apima ir prašymą klientui pačiam nurodyti viešuosius šaltinius, kuriuose informacija apie naudos gavėją galėtų būti patvirtinta. 6.4. Pateiktų duomenų teisingumą klientas patvirtina parašu ir (arba) antspaudu (jeigu jis antspaudą privalo turėti pagal jo veiklą reguliuojančius teisės aktus). 6.5. Jeigu kliento tapatybė nustatoma klientui fiziškai nedalyvaujant, klientas – fizinis asmuo arba kliento – juridinio asmens atstovas privalo pateikti Politikos 6.2. punkte nurodytus duomenis apie naudos gavėją. Kliento pateikti duomenys patvirtinami naudojant Europos Sąjungoje išduotas elektroninės atpažinties priemones, veikiančias pagal aukšto arba pakankamo saugumo užtikrinimo lygio elektroninės atpažinties schemas, arba kvalifikuotu elektroniniu parašu, naudojant kvalifikuotą elektroninio parašo sertifikatą, kuris atitinka Reglamento (ES) 910/2014 reikalavimus, arba naudojant elektronines priemones, leidžiančias tiesioginį vaizdo perdavimą, arba parašu rašytinės formos dokumente. 6.6. Bendrovė privalo kaupti ir FNTT reikalavimu pateikti šiuos duomenis apie naudos gavėją: 6.6.1. naudos gavėjo tapatybės duomenis; 6.6.2. kliento pateiktos informacijos tikrinimo patikimuose ir nepriklausomuose šaltiniuose įrodymus; 6.6.3. duomenis apie kliento (juridinio asmens) nuosavybės ir kontrolės struktūrą. 6.7. Naudos gavėjo tapatybė turi būti nustatyta iki kliento tapatybės nustatymo procedūros pabaigos. 6.8. Nustatant naudos gavėjo tapatybę, papildomai privalo būti gauta informacija iš Juridinių asmenų dalyvių informacinės sistemos (JADIS), iš kurios turi gauti duomenis apie to kliento naudos gavėjus. Bendrovė taip pat turi teisę naudotis kitomis valstybės informacinėmis sistemomis, registrais, kuriuose kaupiami duomenys apie juridinių asmenų dalyvius.	independent sources. Such actions may include requesting the Customer to identify public sources where information about the Beneficial Owner can be verified. 6.4. The Customer shall confirm the accuracy of the provided data by signature and/or seal, where the Customer is required to have a seal under the laws governing its activities. 6.5. Where the Customer is identified remotely, the Customer who is a natural person or the representative of a legal entity Customer shall provide the data regarding the Beneficial Owner specified in Clause 6.2 of this Policy. The data provided by the Customer shall be confirmed by using electronic identification means issued in the European Union and operating under electronic identification schemes with a high or substantial level of assurance, by a qualified electronic signature using a qualified certificate for electronic signatures compliant with Regulation (EU) No 910/2014, by using electronic means enabling live video transmission, or by signature on a written document. 6.6. The Company shall collect and, at the request of the FCIS, provide the following data regarding the Beneficial Owner: 6.6.1. identification data of the Beneficial Owner; 6.6.2. evidence of verification of the information provided by the Customer against reliable and independent sources; 6.6.3. data regarding the ownership and control structure of the Customer that is a legal entity. 6.7. The Beneficial Owner must be identified before completion of the Customer identification procedure. 6.8. When identifying the Beneficial Owner, information must additionally be obtained from the Information System of Legal Entity Participants (JADIS), including data on the Beneficial Owners of the relevant Customer. The Company may also use other state information systems and registers containing data on participants of legal entities. Where the Employee
---	--



Nustačius informacijos apie kliento – juridinio asmens naudos gavėjus, pateiktos Juridinių asmenų dalyvių informacinėje sistemoje (JADIS), ir jų turimos informacijos apie to paties kliento naudos gavėjus neatitiktį, Darbuotojas turi pranešti apie tai klientui ir pasiūlyti pateikti tikslią informaciją apie savo naudos gavėjus Juridinių asmenų dalyvių informacinės sistemos (JADIS) tvarkytojui. Kol kliento pateikta informacija skiriasi nuo Juridinių asmenų dalyvių informacinėje sistemoje (JADIS) skelbiamos informacijos, ar jei Juridinių asmenų dalyvių informacinės sistemos (JADIS) nėra pateikiama duomenų apie kliento naudos gavėjus, dalykiniai santykiai su klientu nepradedami.	identifies a discrepancy between the information on the Beneficial Owners of the legal entity Customer provided in JADIS and the information available to the Company regarding the same Customer's Beneficial Owners, the Employee shall notify the Customer and propose that accurate information on the Beneficial Owners be submitted to the administrator of JADIS. Until the information provided by the Customer corresponds to the information published in JADIS, or where JADIS contains no data on the Customer's Beneficial Owners, no business relationship with the Customer shall be established.
7. SUSTIPRINTAS KLIENTO TAPATYBĖS NUSTATYMAS	7. ENHANCED CUSTOMER DUE DILIGENCE
7.1. Prieš kliento tapatybės nustatymo procedūrą Darbuotojas patikrina, ar yra aplinkybių taikyti sustiprintą kliento tapatybės nustatymą.	7.1. Before carrying out the Customer identification procedure, the Employee shall verify whether there are circumstances requiring the application of Enhanced Customer Due Diligence.
7.2. Sustiprintas kliento tapatybės nustatymas atliekamas:	7.2. Enhanced Customer Due Diligence shall be carried out:
7.2.1. kai sandoriai ar dalykiniai santykiai atliekami su politiškai pažeidžiamais (paveikiamais) asmenimis;	7.2.1. where transactions or business relationships are conducted with Politically Exposed Persons (PEPs);
7.2.2. jeigu, vertinant Politikos 7.8. punkte nurodytus veiksnius, nustatoma didesnė pinigų plovimo ir (ar) teroristų finansavimo rizika. Jei klientas atitinka bent vieną Politikos 7.8. punkte nurodytą veiksnį, jis laikomas keliančiu didesnę pinigų plovimo ir (ar) teroristų finansavimo riziką;	7.2.2. where, upon assessment of the factors set out in Clause 7.8 of this Policy, a higher money laundering and/or terrorist financing risk is identified. If the Customer meets at least one of the factors specified in Clause 7.8, the Customer shall be deemed to pose a higher money laundering and/or terrorist financing risk;
7.2.3. kai sandoriai ar dalykiniai santykiai atliekami su Europos Komisijos nustatytose didelės rizikos trečiosiose valstybėse gyvenančiais fiziniais asmenimis ar ten įsteigtais juridiniais asmenimis. Įvertinus riziką, sustiprinto kliento tapatybės nustatymo priemonės neprivalo būti taikomos Europos Sąjungoje įsisteigusių finansų įstaigų ar kitų įpareigotųjų subjektų filialams ar patronuojamosioms įmonėms,	7.2.3. where transactions or business relationships are conducted with natural persons residing in, or legal entities established in, high-risk third countries identified by the European Commission. Following a risk assessment, Enhanced Customer Due Diligence measures need not be applied to branches or majority-owned subsidiaries of financial institutions or other obliged entities established in the European

kuriuose jie turi daugumą akcijų ir kurie yra Europos Komisijos nustatytoje didelės rizikos trečiojoje valstybėje, jeigu tie filialai ar patronuojamosios įmonės laikosi visos grupės nustatytų reikalavimų, lygiaverčių šio įstatymo reikalavimams; 7.2.4. kai sandoriai ar dalykiniai santykiai atliekami su pagal Finansinių veiksmų darbo grupės kovai su pinigų plovimu ir teroristų finansavimu skelbiamus valstybių, turinčių rimtų trūkumų dėl pinigų plovimo ir (ar) teroristų finansavimo prevencijos ir šių nusikaltimų užkardymo, sąrašus nustatytoje didelės rizikos trečiojoje valstybėje gyvenančiais fiziniais asmenimis ar ten įsteigtais juridiniais asmenimis. 7.3. Atlikdami sustiprintą kliento tapatybės nustatymą, kai dalykiniai santykiai atliekami su politiškai pažeidžiamais (paveikiamais) asmenimis, Darbuotojas privalo: 7.3.1. patikrinti ar šis asmuo, jo atstovas, naudos gavėjas ar jų artimieji šeimos nariai bei artimi pagalbininkai yra politiškai pažeidžiami (paveikiami) asmenys arba tokiais buvo per pastaruosius 12 mėn.; 7.3.2. patikrinti Politikos 7.3.1. papunktyje nurodytą informaciją apie klientą bei jo atstovą, naudos gavėją ar jų artimuosius šeimos narius bei artimus pagalbininkus patikimuose viešosiose paieškos šaltiniuose; 7.3.3. patikrinti kokius atsakymus dėl politiškai pažeidžiamų (paveikiamų) asmenų klientas nurodė anketoje; 7.3.4. imtis atitinkamų priemonių turto ir lėšų, susijusių su dalykiniais santykiais arba sandoriu, šaltiniui nustatyti – paprašyti kliento paaiškinti iš kur klientas turi šias lėšas bei pateikti dokumentus, pagrindžiančius kliento teiginius, kai Darbuotojo manymu tai yra būtina; 7.3.5. gauti Bendrovės direktoriaus pritarimą dalykiniams santykiams su tokiais klientais užmegzti ar tęsti dalykinius santykius su klientais, kai jie tampa politiškai pažeidžiami (paveikiami)	Union and located in high-risk third countries identified by the European Commission, provided that such branches or subsidiaries comply with group-wide requirements equivalent to the requirements of the AML/CFT Law; 7.2.4. where transactions or business relationships are conducted with natural persons residing in, or legal entities established in, high-risk third countries identified in the lists published by the Financial Action Task Force (FATF) of countries with strategic deficiencies in their anti-money laundering and/or counter-terrorist financing systems. 7.3. When applying Enhanced Customer Due Diligence in relation to business relationships with Politically Exposed Persons, the Employee shall: 7.3.1. verify whether the Customer, the Customer's representative, the Beneficial Owner, or their Close Family Members or Close Associates are Politically Exposed Persons or have been Politically Exposed Persons during the preceding twelve (12) months; 7.3.2. verify the information referred to in Clause 7.3.1 regarding the Customer, the Customer's representative, the Beneficial Owner, or their Close Family Members or Close Associates using reliable public sources; 7.3.3. check the answers provided by the Customer in the questionnaire regarding Politically Exposed Persons; 7.3.4. take appropriate measures to establish the source of wealth and source of funds related to the business relationship or transaction, including by requesting the Customer to explain the origin of such funds and, where the Employee considers it necessary, to provide documents supporting the Customer's statements; 7.3.5. obtain the approval of the Company's Director to establish business relationships with such Customers or to continue business relationships with Customers who become
--	--

asmenys. 7.3.6. vykdyti sustiprintą nuolatinę dalykinių santykių su politiškai pažeidžiamais (paveikiamais) fiziniais asmenimis stebėseną. 7.4. Kai politiškai pažeidžiamas (paveikiamas) asmuo nustoja eiti svarbias viešąsias pareigas, Bendrovė ne trumpesnę kaip 12 mėnesių laikotarpį privalo toliau atsižvelgti į to asmens tebekeliamą riziką ir taikyti tinkamas pagal rizikos lygį pritaikytas priemones tol, kol nustatoma, kad tas asmuo nebekelia politiškai pažeidžiamiems (paveikiamiems) asmenims būdingos rizikos. 7.5. Bendrovė, įgyvendindama šiame skyriuje nustatytus reikalavimus, turi teisę gauti iš Vyriausiosios tarnybinės etikos komisijos turimus asmenų, kurie yra politiškai pažeidžiami (paveikiami), kuriems patikėtos svarbios viešosios pareigos Lietuvos Respublikoje, kurie teisės aktų nustatyta tvarka turi prievolę deklaruoti savo viešuosius bei privačius interesus ir kurių deklaracijų duomenys yra vieši, privačių interesų deklaracijų duomenis. Patikrą galima atlikti paspaudus šią nuorodą https://pinreg.vtek.lt/app/. 7.6. Taikydami sustiprintą kliento tapatybės nustatymą, kai sandoriai ar dalykiniai santykiai atliekami su Europos Komisijos nustatytoje didelės rizikos trečiosiose valstybėse gyvenančiais fiziniais asmenimis ar ten įsteigtais juridiniais asmenimis, Darbuotojas privalo: 7.6.1. gauti papildomos informacijos apie klientą ir naudos gavėją; 7.6.2. gauti papildomos informacijos apie numatomą verslo santykių pobūdį; 7.6.3. gauti informacijos apie kliento ir naudos gavėjo lėšų ir turto šaltinį; 7.6.4. gauti informacijos apie numatomų arba įvykdytų sandorių priežastis; 7.6.5. gauti direktoriaus pritarimą užmegzti dalykinius santykius su šiais klientais ar pritarimą tęsti dalykinius santykius su šiais klientais; 7.6.6. vykdyti sustiprintą nuolatinę dalykinių santykių su šiais Klientais stebėseną, padidindami	Politically Exposed Persons; 7.3.6. conduct enhanced ongoing monitoring of business relationships with Politically Exposed Persons. 7.4. Where a Politically Exposed Person ceases to hold prominent public functions, the Company shall, for a period of at least twelve (12) months, continue to take into account the ongoing risk posed by that person and apply appropriate risk-sensitive measures until it determines that the person no longer poses risks characteristic of Politically Exposed Persons. 7.5. In implementing the requirements set out in this Section, the Company shall have the right to obtain from the Chief Official Ethics Commission data contained in declarations of private interests of persons who are Politically Exposed Persons, who have been entrusted with prominent public functions in the Republic of Lithuania, who are required by law to declare their public and private interests, and whose declaration data are public. 7.6. When applying Enhanced Customer Due Diligence in cases where transactions or business relationships are conducted with natural persons residing in, or legal entities established in, high-risk third countries identified by the European Commission, the Employee shall: 7.6.1. obtain additional information about the Customer and the Beneficial Owner; 7.6.2. obtain additional information about the intended nature of the business relationship; 7.6.3. obtain information about the source of funds and source of wealth of the Customer and the Beneficial Owner; 7.6.4. obtain information on the reasons for the intended or completed transactions; 7.6.5. obtain the Director's approval to establish or continue business relationships with such Customers; 7.6.6. conduct enhanced ongoing monitoring of business relationships with such Customers by
--	--

taikomų kontrolės priemonių skaičių ir terminus ir atrinkdami sandorių, kuriems reikės tolesnio ištyrimo, tipus; 7.6.7. užtikrinti, kad pirmasis kliento mokėjimas būtų atliekamas iš kredito, mokėjimo ar elektroninių pinigų įstaigoje turimos to kliento sąskaitos, kai kredito, mokėjimo ar elektroninių pinigų įstaiga yra registruota Europos Sąjungos valstybėje narėje arba trečiojoje valstybėje, nustačiusioje PPTFPĮ reikalavimams lygiaverčius reikalavimus, ir kompetentingos institucijos prižiūri, kaip ji šių reikalavimų laikosi. 7.7. Taikydami sustiprintą kliento tapatybės nustatymą tais atvejais, kai sandoriai ar dalykiniai santykiai atliekami su pagal Finansinių veiksmų darbo grupės kovai su pinigų plovimu ir teroristų finansavimu skelbiamuose valstybių, turinčių rimtų trūkumų dėl pinigų plovimo ir (ar) teroristų finansavimo prevencijos ir šių nusikaltimų užkardymo, sąrašus nustatytoje didelės rizikos trečiosiose valstybėse gyvenančiais fizineis asmenimis bei tais atvejais, kai pagal Bendrovės rizikos vertinimo ir valdymo procedūras nustatoma didesnė pinigų plovimo ir (ar) teroristų finansavimo rizika, Darbuotojas imasi vienos ar kelių papildomų kliento ir naudos gavėjo tapatybės nustatymo priemonių kylančiai rizikai mažinti ir privalo: 7.7.1. gauti direktoriaus pritarimą užmegzti dalykinius santykius su šiais klientais ar pritarimą tęsti dalykinius santykius su šiais klientais; 7.7.2. paprašyti pateikti išsamius paaiškinimus apie naudos gavėją bei jo vykdomą veiklą už Lietuvos Respublikos ribų, turtą arba lėšas, susijusias su dalykiniais santykiais; 7.7.3. vykdyti sustiprintą nuolatinę dalykinių santykių su šiais klientais stebėseną. 7.8. Bendrovės darbuotojai, nustatydami, ar egzistuoja didesnė pinigų plovimo ir (ar) teroristų finansavimo rizika, privalo vertinti bent jau šiuos veiksniai: 7.8.1. kliento požymius: 7.8.1.1. kliento dalykiniai santykiai vykdomi	increasing the number and frequency of controls applied and selecting transaction patterns requiring further examination; 7.6.7. ensure that the Customer's first payment is made from an account held in the Customer's name with a credit institution, payment institution or electronic money institution established in a Member State of the European Union or in a third country that has established requirements equivalent to those of the AML/CFT Law and is supervised by competent authorities for compliance with such requirements. 7.7. When applying Enhanced Customer Due Diligence in cases where transactions or business relationships are conducted with natural persons residing in, or legal entities established in, high-risk third countries identified in the lists published by the Financial Action Task Force (FATF) of countries with strategic deficiencies in their anti-money laundering and/or counter-terrorist financing systems, and in cases where a higher money laundering and/or terrorist financing risk is identified under the Company's risk assessment and management procedures, the Employee shall apply one or more additional Customer and Beneficial Owner identification measures to mitigate the risks and shall: 7.7.1. obtain the Director's approval to establish or continue business relationships with such Customers; 7.7.2. request detailed explanations regarding the Beneficial Owner and the Beneficial Owner's activities outside the Republic of Lithuania, as well as the assets or funds related to the business relationship; 7.7.3. conduct enhanced ongoing monitoring of business relationships with such Customers. 7.8. When determining whether a higher money laundering and/or terrorist financing risk exists, the Company's Employees shall assess at least the following factors: 7.8.1. Customer risk factors: 7.8.1.1. the Customer's business relationship is
---	---

nejprastomis aplinkybėmis be akivaizdaus ekonominio ar matomo teisėto tikslo; 7.8.1.2. už klientą moka kiti asmenys ir tam nėra jokio logiško paaiškinimo; 7.8.1.3. klientas gyvena trečiojoje valstybėje; 7.8.1.4. juridiniai asmenys ar juridinio asmens statuso neturintys subjektai vykdo asmeninės turto valdymo įmonės veiklą; 7.8.1.5. Klientas turi formalių akcininkų, veikiančių už kitą asmenį, arba pareikštinės formos akcijų; 7.8.2. produkto, paslaugos, sandorio ar paslaugų teikimo kanalo požymius: 7.8.2.1. sudaromas sandoris, kurio įvykdymui užtikrinti įkeičiamas trečiojo, su klientu ar naudos gavėju nesusijusio asmens turtas ir klientas nepateikia racionalaus paaiškinimo kodėl toks sandoris sudaromas; 7.8.2.2. mokėjimai gauti iš nežinomų arba nesusijusių trečiųjų šalių; 7.8.3. teritorijos požymius: 7.8.3.1. remiantis Finansinių veiksmų darbo grupės kovai su pinigų plovimu ir teroristų finansavimu arba panašaus pobūdžio regioninės organizacijos ataskaitų ar panašių dokumentų duomenimis, valstybėje nustatyta reikšmingų kovos su pinigų plovimu ir teroristų finansavimu sistemos neatitikčių tarptautiniams reikalavimams; 7.8.3.2. remiantis vyriausybinių ir visuotinai pripažintų nevyriausybinių organizacijų, stebinių ir vertinančių korupcijos lygį, duomenimis, valstybėje nustatytas didelis korupcijos ar kitos nusikalstamos veiklos lygis; 7.8.3.3. valstybei taikomos sankcijos, embargas ar panašios priemonės, paskelbtos, pavyzdžiui, Europos Sąjungos arba Jungtinių Tautų; 7.8.3.4. valstybė finansuoja arba remia teroristų veiklą arba valstybių teritorijoje veikia į tarptautinių organizacijų sudarytus sąrašus įtrauktos teroristų organizacijos.	conducted in unusual circumstances without an apparent economic or visible lawful purpose; 7.8.1.2. payments are made on behalf of the Customer by other persons without any logical explanation; 7.8.1.3. the Customer resides in a third country; 7.8.1.4. legal entities or legal arrangements operate as personal asset-holding vehicles; 7.8.1.5. the Customer has nominee shareholders acting on behalf of another person or bearer shares; 7.8.2. Product, service, transaction or delivery channel risk factors: 7.8.2.1. a transaction is concluded where performance is secured by collateral provided by a third party unrelated to the Customer or the Beneficial Owner, and the Customer does not provide a reasonable explanation for such transaction; 7.8.2.2. payments are received from unknown or unrelated third parties; 7.8.3. Geographic risk factors: 7.8.3.1. based on reports or similar documents issued by the Financial Action Task Force (FATF) or a similar regional body, the country has significant deficiencies in its anti-money laundering and counter-terrorist financing framework in relation to international requirements; 7.8.3.2. based on information from governmental and widely recognised non-governmental organisations monitoring and assessing corruption levels, the country has a high level of corruption or other criminal activity; 7.8.3.3. the country is subject to sanctions, embargoes or similar measures imposed, for example, by the European Union or the United Nations; 7.8.3.4. the country finances or supports terrorist activities, or terrorist organisations included in lists compiled by international organisations operate within its territory.
--	---

8. SUPAPRASTINTAS TAPATYBĖS NUSTATYMAS 8.1. Supaprastintas kliento tapatybės nustatymas atliekamas tais atvejais, kai kliento bendra per kalendorinius metus Bendrovės administruojamoje sutelktinio finansavimo platformoje Revestus investuojama / ketinama investuoti suma neviršija 30 000,00 EUR ir sukaupta palūkanų ar kita mokėtina suma grąžinama tik į kliento kredito, mokėjimo ar elektroninių pinigų įstaigoje turimą sąskaitą, iš kurios buvo pervedamos lėšos, taip pat kai klientas priskiriamas mažą riziką keliančių klientų grupei. 8.2. Taikydama supaprastintą kliento tapatybės nustatymą, Bendrovė: 8.2.1. surenka šiuos duomenis: 8.2.1.1. iš kliento – fizinio asmens: vardas (vardai), pavardė (pavardės), asmens kodas (užsieniečiui – gimimo data (jeigu yra – asmens kodas ar kita šiam asmeniui suteikta unikali simbolių seka, skirta asmeniui identifikuoti), leidimo gyventi Lietuvos Respublikoje numeris ir galiojimo laikas, jo išdavimo vieta ir data (taikoma užsieniečiams); 8.2.1.2. iš kliento – juridinio asmens: pavadinimas, teisinė forma, buveinė, faktinės veiklos vykdymo adresas, kodas (jei toks yra suteiktas). 8.2.2. užtikrina, kad pirmasis kliento mokėjimas būtų atliekamas iš kredito, mokėjimo ar elektroninių pinigų įstaigoje turimos sąskaitos, kai kredito, mokėjimo ar elektroninių pinigų įstaiga yra registruota Europos Sąjungos valstybėje narėje arba Trečiojoje valstybėje, nustačiusioje PPTFPJ reikalavimams lygiavertčius reikalavimus, ir kompetentingos institucijos prižiūri, kaip ji šių reikalavimų laikosi. 8.3. Bendrovė netaiko supaprastinto tapatybės nustatymo, jeigu yra šios Politikos 7 skyriuje nurodytos aplinkybės, kai būtina atlikti sustiprintą kliento tapatybės nustatymą. 8.4. Jeigu vykdant nuolatinę kliento dalykinių	8. SIMPLIFIED CUSTOMER DUE DILIGENCE 8.1. Simplified Customer Due Diligence shall be applied where the Customer's total amount invested or intended to be invested through the crowdfunding platform Revestus administered by the Company during a calendar year does not exceed EUR 30,000, and all accrued interest or any other amounts payable are repaid only to the Customer's account held with a credit institution, payment institution or electronic money institution from which the funds were originally transferred, provided that the Customer is classified as a low-risk Customer. 8.2. When applying Simplified Customer Due Diligence, the Company shall: 8.2.1. collect the following information: 8.2.1.1. from a Customer who is a natural person: first name(s), surname(s), personal identification number (or, for a foreign national, date of birth and, where available, a personal identification number or other unique identifier assigned to the individual), residence permit number in the Republic of Lithuania (where applicable), its validity period, place and date of issue (applicable to foreign nationals); 8.2.1.2. from a Customer who is a legal entity: name, legal form, registered office, actual place of business, and registration number (where applicable). 8.2.2. ensure that the Customer's first payment is made from an account held in the Customer's name with a credit institution, payment institution or electronic money institution established in a Member State of the European Union or in a third country that has established requirements equivalent to those of the AML/CFT Law and is supervised by the competent authorities for compliance with such requirements. 8.3. The Company shall not apply Simplified Customer Due Diligence where any of the circumstances specified in Section 7 of this Policy requiring Enhanced Customer Due Diligence are present. 8.4. Where, during the ongoing monitoring of the
---	--

santykių stebėseną nustatoma, kad pinigų plovimo ir (ar) teroristų finansavimo rizika nebėra maža, Bendrovė privalo imtis šioje Politikoje nustatytų priemonių ir nustatyti bei patikrinti ir kliento, ir naudos gavėjo tapatybę.	Customer's business relationship, it is established that the money laundering and/or terrorist financing risk is no longer low, the Company shall apply the measures set out in this Policy to identify and verify both the Customer and the Beneficial Owner.
9. DALYKINIŲ SANTYKIŲ STEBĖSENA IR TARPTAUTINIŲ FINANSINIŲ SANKCIJŲ IR RIBOJAMŲJŲ PRIEMONIŲ ĮGYVENDINIMAS	9. ONGOING MONITORING OF BUSINESS RELATIONSHIPS AND IMPLEMENTATION OF INTERNATIONAL FINANCIAL SANCTIONS AND RESTRICTIVE MEASURES
9.1. Užmezgusi su klientais dalykinius santykius, Bendrovė vykdo įprastą arba sustiprintą nuolatinę operacijų (sandorių) ir šių Klientų dalykinių santykių stebėseną:	9.1. Once business relationships with Customers have been established, the Company shall conduct either standard or enhanced ongoing monitoring of transactions and business relationships:
9.1.1. įprasta operacijų (sandorių) ir dalykinių santykių stebėseną vykdoma klientų, kurių tapatybei nustatyti buvo pasitelktos šioje Politikoje numatytos įprastos klientų tapatybės nustatymo procedūros. Šiuo atveju vykdoma nuolatinė klientų operacijų stebėseną ir, tuo atveju jeigu nekyla įtarimų, klientų pateikti duomenys ir jų patikrinimo nepriklausomuose šaltiniuose duomenys peržiūrimi ir atnaujinami periodiškai, tačiau ne rečiau kaip kartą per metus;	9.1.1. standard monitoring shall be carried out in respect of Customers whose identity has been established using the standard Customer Due Diligence procedures provided for in this Policy. In such cases, the Company shall perform continuous monitoring of Customer transactions and, where no suspicions arise, the Customer's information and the information obtained from independent sources shall be reviewed and updated periodically, but at least once per year;
9.1.2. sustiprinta operacijų (sandorių) ir dalykinių santykių stebėseną vykdoma klientų, kurių tapatybei nustatyti buvo pasitelktos šioje Politikoje numatytos sustiprintos kliento tapatybės nustatymo procedūros. Šiuo atveju vykdoma nuolatinė klientų operacijų stebėseną ir tuo atveju, jeigu nekyla įtarimų, klientų pateikti duomenys ir jų patikrinimo nepriklausomuose šaltiniuose duomenys peržiūrimi ir atnaujinami periodiškai, tačiau ne rečiau kaip du kartus per metus.	9.1.2. enhanced monitoring shall be carried out in respect of Customers whose identity has been established using the Enhanced Customer Due Diligence procedures provided for in this Policy. In such cases, the Company shall perform continuous monitoring of Customer transactions and, where no suspicions arise, the Customer's information and the information obtained from independent sources shall be reviewed and updated periodically, but at least twice per year.
9.2. Vykdydama nuolatinę operacijų (sandorių) ir klientų dalykinių santykių stebėseną (tiek įprastą, tiek sustiprintą), Bendrovė visais atvejais:	9.2. In conducting ongoing monitoring of transactions and Customer business relationships (whether standard or enhanced), the Company shall in all cases:
9.2.1. atlieka duomenų apie klientų, jų atstovų bei naudos gavėjų tapatybės peržiūrą;	9.2.1. review the identification information relating to Customers, their representatives and

9.2.2. atlieka sandorių, kurie buvo sudaryti dalykinių santykių metu, patikrinimus, siekiant užtikrinti, kad vykdomi sandoriai atitiktų Bendrovės turimas žinias apie klientą, jo verslą, rizikos pobūdį ir žinias apie lėšų šaltinį; 9.2.3. nedelsiant imasi priemonių, kad būtų užkirstas kelias pinigų plovimui ir (arba) teroristų finansavimui. 9.3. Bendrovės darbuotojams nustačius, kad klientas ar naudos gavėjas yra įtraukti į šios Politikos 3.6.3. punkte nurodytus sąrašus dalykinių santykių metu, Bendrovės darbuotojai: 9.3.1. nedelsiant nutraukia prievolių, atsiradusių iki nustatant, kad klientas ar naudos gavėjas yra įtraukti į šios Politikos 3.6.3. punkte nurodytus sąrašus, įgyvendinimą, vykdymą, arba sustabdo jų vykdymą; 9.3.2. nedelsiant vienašališkai nutraukia sandorius, kurie buvo sudaryti iki nustatant, kad klientas ar naudos gavėjas yra įtraukti į šios Politikos 3.6.3. punkte nurodytus sąrašus, arba sustabdo jų vykdymą; 9.3.3. apie tai per 3 valandas informuoja FNTT; 9.3.4. pateikia FNTT visus priežiūrai atlikti reikalingus duomenis. 10. PRANEŠIMAS APIE ĮTARTINAS PINIGINES OPERACIJAS AR SANDORIUS 10.1. Pranešimą su informacija apie įtartinas pinigines operacijas arba sandorius FNTT Darbuotojas pateikia elektroniniu paštu. Darbuotojas privalo FNTT nurodyti: 10.1.1. kliento, jo atstovo (jeigu piniginė operacija atliekama per atstovą) tapatybę patvirtinančius duomenis (fizinio asmens – vardas, pavardė, asmens kodas (užsieniečiui – gimimo data, jeigu yra – asmens kodas ar kita šiam asmeniui suteikta unikali simbolių seka, skirta asmeniui	Beneficial Owners; 9.2.2. review transactions carried out during the business relationship to ensure that such transactions are consistent with the Company's knowledge of the Customer, the Customer's business, risk profile and source of funds; 9.2.3. immediately take appropriate measures to prevent money laundering and/or terrorist financing. 9.3. Where the Company's Employees establish during the course of a business relationship that the Customer or the Beneficial Owner has been included in the sanctions lists referred to in Clause 3.6.3 of this Policy, the Employees shall: 9.3.1. immediately terminate or suspend the performance of obligations arising before it was established that the Customer or the Beneficial Owner had been included in the sanctions lists referred to in Clause 3.6.3 of this Policy; 9.3.2. immediately terminate unilaterally or suspend the performance of any agreements concluded before it was established that the Customer or the Beneficial Owner had been included in the sanctions lists referred to in Clause 3.6.3 of this Policy; 9.3.3. notify the Financial Crime Investigation Service (FCIS) within three (3) hours; 9.3.4. provide the FCIS with all information necessary for supervisory purposes. 10. REPORTING OF SUSPICIOUS MONETARY TRANSACTIONS OR TRANSACTIONS 10.1. An Employee shall submit a report containing information on suspicious monetary transactions or transactions to the Financial Crime Investigation Service (FCIS) by email. The Employee shall provide the FCIS with the following information: 10.1.1. identification data of the Customer and, where the monetary transaction is carried out through a representative, the Customer's representative (for a natural person: first name, surname, personal identification number (or, for a foreign national, date of birth and, where
---	--

identifikuoti), juridinio asmens – pavadinimas, teisinė forma, buveinės adresas, kodas, jeigu toks kodas suteiktas); 10.1.2. kokį FNTT patvirtintą kriterijų, nustatytą Politikos 1.2.5. papunktyje nurodytame teisės akte, operacija atitinka; 10.1.3. įtartinos piniginės operacijos atlikimo būdą, jei pranešama apie įtartiną piniginę operaciją; 10.1.4. įtartinos piniginės operacijos ar sandorio atlikimo datą ir jo vertę; 10.1.5. kliento, jo atstovo (jeigu piniginė operacija atliekama per atstovą) kontaktinę informaciją (telefono numeriai, elektroninio pašto adresai, kontaktiniai asmenys, jų telefono numeriai, elektroninio pašto adresai); 10.1.6. subjektą, kurio naudai atliekama įtartina piniginė operacija ar sudarytas sandoris (fizinio asmens – vardas, pavardė, asmens kodas (užsieniečiui – gimimo data, jeigu yra – asmens kodas ar kita šiam asmeniui suteikta unikali simbolių seka, skirta asmeniui identifikuoti), juridinio asmens – pavadinimas, teisinė forma, buveinės adresas, kodas); 10.1.7. įtartinos piniginės operacijos sustabdymo datą ir laiką; 10.1.8. jeigu įtartina piniginė operacija nebuvo stabdomi, – priežastis, dėl kurių jie nestabdyti; 10.1.9. kitą, Darbuotojo nuomone, svarbią informaciją. 10.2. Darbuotojai privalo nedelsdami, ne vėliau kaip per 1 darbo dieną nuo tokių žinių ar įtarimų atsiradimo, pranešti direktoriui ir FNTT, jeigu žino ar įtaria, kad bet kokia lėšų suma yra tiesiogiai arba netiesiogiai gauta iš nusikalstamos veikos arba dalyvaujant tokioje veikoje, taip pat jeigu žino ar įtaria, kad lėšos yra skirtos vienam, keliems teroristams ar teroristinei organizacijai remti.	available, a personal identification number or other unique identifier assigned to the person); for a legal entity: name, legal form, registered office address and registration number, where applicable); 10.1.2. the criterion approved by the FCIS and referred to in Clause 1.2.5 of this Policy that the transaction meets; 10.1.3. the method by which the suspicious monetary transaction was carried out, where the report concerns a suspicious monetary transaction; 10.1.4. the date and value of the suspicious monetary transaction or transaction; 10.1.5. contact details of the Customer and, where applicable, the Customer's representative (telephone number, email address, contact persons, their telephone numbers and email addresses); 10.1.6. the person for whose benefit the suspicious monetary transaction is carried out or the transaction has been concluded (for a natural person: first name, surname, personal identification number (or, for a foreign national, date of birth and, where available, a personal identification number or other unique identifier assigned to the person); for a legal entity: name, legal form, registered office address and registration number); 10.1.7. the date and time when the suspicious monetary transaction was suspended; 10.1.8. where the suspicious monetary transaction was not suspended, the reasons why it was not suspended; 10.1.9. any other information that, in the Employee's opinion, may be relevant. 10.2. Employees shall immediately, and no later than within one (1) business day after becoming aware of or suspecting such circumstances, notify both the Company's Director and the FCIS if they know or suspect that any amount of funds has been obtained, directly or indirectly, from criminal activity or participation therein, or if they know or suspect that the funds are intended to
---	--



10.3. Bendrovės darbuotojai nustatę, kad klientas atlieka įtartiną piniginę operaciją, nepaisydami piniginės operacijos sumos, privalo tą operaciją sustabdyti ir ne vėliau kaip per 3 darbo valandas nuo piniginės operacijos sustabdymo apie šią operaciją pranešti direktoriui ir FNTT. 10.4. Darbuotojai, gavę informacijos, kad klientas ketina ar bandys atlikti įtartiną piniginę operaciją, privalo nedelsdami informuoti direktorių ir FNTT. 10.5. Bendrovė, gavusi iš FNTT rašytinį nurodymą sustabdyti kliento atliekamas įtartinas pinigines operacijas ar sandorius, privalo nuo jame nurodyto laiko ar konkrečių aplinkybių atsiradimo momento iki 10 darbo dienų sustabdyti šias operacijas ar sandorius. 10.6. Jeigu Bendrovė per 10 darbo dienų nuo pranešimo pateikimo ar nurodymo gavimo nėra įpareigojami vykdyti laikino nuosavybės teisių apribojimo Lietuvos Respublikos baudžiamojo proceso kodekso (toliau – Baudžiamojo proceso kodeksas) nustatyta tvarka, piniginė operacija ar sandoris turi būti atnaujinami. Anksčiau šio termino pasibaigimo piniginės operacijos gali būti atnaujinamos tik esant rašytiniam FNTT nurodymui. 10.7. Gavus FNTT pranešimą, kad sustabdyta kliento atliekama įtartina piniginė operacija turi būti atlikta, Darbuotojas nedelsiant atlieka veiksmus, kad būtų nutrauktas įtartinos piniginės operacijos sustabdymas. 10.8. Bendrovė privalo pateikti FNTT prašomą informaciją per 1 darbo dieną nuo prašymo gavimo momento. 11. KLIENTŲ SKIRSTYMAS Į RIZIKOS GRUPES 11.1. Bendrovė Klientus skirsto į šias grupes:	support one or more terrorists or a terrorist organisation. 10.3. Where Company Employees determine that a Customer is carrying out a suspicious monetary transaction, they shall, irrespective of the amount involved, suspend the transaction and notify both the Company's Director and the FCIS no later than three (3) business hours after the suspension. 10.4. Employees who receive information indicating that a Customer intends or attempts to carry out a suspicious monetary transaction shall immediately notify the Company's Director and the FCIS. 10.5. Upon receipt of a written instruction from the FCIS to suspend suspicious monetary transactions or transactions carried out by a Customer, the Company shall suspend such transactions from the time or occurrence of the circumstances specified in the instruction for a period of up to ten (10) business days. 10.6. Where, within ten (10) business days following the submission of the report or receipt of the FCIS instruction, no temporary restriction of property rights is imposed in accordance with the procedure established by the Code of Criminal Procedure of the Republic of Lithuania (the "Code of Criminal Procedure"), the monetary transaction or transaction shall be resumed. Prior to the expiry of that period, transactions may only be resumed upon receipt of written instructions from the FCIS. 10.7. Upon receipt of a notification from the FCIS that a suspended suspicious monetary transaction shall be executed, the Employee shall immediately take the necessary steps to terminate the suspension of that transaction. 10.8. The Company shall provide the FCIS with any information requested within one (1) business day of receipt of such request. 11. CUSTOMER RISK CLASSIFICATION 11.1. The Company shall classify Customers into the following risk categories:
--	--

11.1.1. keliančius mažą pinigų plovimo ir (ar) teroristų finansavimo grėsmę; 11.1.2. keliančius vidutinę pinigų plovimo ir (ar) teroristų finansavimo grėsmę; ir 11.1.3. keliančius didelę pinigų plovimo ir (ar) teroristų finansavimo grėsmę. 11.2. Bendrovės klientai priskiriami prie keliančių vidutinę pinigų plovimo ir (ar) teroristų finansavimo grėsmę Klientų grupės, išskyrus tuos atvejus kai: 11.2.1. yra pagrindas juos priskirti prie keliančių mažą pinigų plovimo ir (ar) teroristų finansavimo grėsmę klientų grupės arba; 11.2.2. yra pagrindas juos priskirti prie keliančių didelę pinigų plovimo ir (ar) teroristų finansavimo grėsmę klientų grupės. 11.3. Klientas priskiriamas rizikos grupei atlikus vertinimą pagal žemiau nurodytus kriterijus:		11.1.1. Customers posing a low money laundering and/or terrorist financing risk; 11.1.2. Customers posing a medium money laundering and/or terrorist financing risk; and 11.1.3. Customers posing a high money laundering and/or terrorist financing risk. 11.2. Customers shall be classified as presenting a medium money laundering and/or terrorist financing risk, except where: 11.2.1. there are grounds to classify them as low-risk Customers; or 11.2.2. there are grounds to classify them as high-risk Customers. 11.3. A Customer shall be assigned to a risk category following an assessment based on the criteria set out below.	
Nr. / No	Kriterijus / Criterion	Reikšmė / Value	Balas / Score
1.	Teisinis statusas / Legal Status	Fizinis asmuo / Natural person	0
		Juridinis asmuo / Legal entity	1
	Rezidento statusas / Residency Status	Kliento rezidavimo šalis / pagrindinio atstovo šalis / akcininko šalis / naudos gavėjo šalis yra Lietuva / The Customer's country of residence / the country of the principal representative / shareholder / beneficial owner is Lithuania	0
		Kliento rezidavimo šalis / pagrindinio atstovo šalis / akcininko šalis / naudos gavėjo šalis yra ne Lietuva / The Customer's country of residence / the country of the principal representative / shareholder / beneficial owner is not Lithuania	1
3.	PEP statusas / PEP Status	Klientas nėra PEP / The Customer is not a Politically Exposed Person (PEP)	0
		Klientas yra PEP / The Customer is a Politically Exposed Person (PEP)	2
4.	Naujas juridinis asmuo / New Legal Entity	Klientas juridinis asmuo įsteigtas daugiau kaip prieš 365 dienas / The Customer (legal entity) was incorporated more than 365 days ago	0
		Klientas juridinis asmuo įsteigtas mažiau kaip prieš 365 dienas / The Customer (legal entity) was incorporated less than 365 days ago	1
5.	Politikos 7.8. punkte	Klienat neatitinka nei vieno Politikos 7.8. nurodytų kriterijų /	0

	nurodytų kriterijų atitikimas / Compliance with the Criteria Set Out in Clause 7.8 of the Policy	The Customer does not meet any of the criteria set out in Clause 7.8 of the Policy	
		Klientas atitinka bent vieną Politikos 7.8. nurodytų kriterijų / The Customer meets at least one of the criteria set out in Clause 7.8 of the Policy	2
11.4. Klientas pagal surinktų balų skaičių priskiriamas šiai rizikos grupei: 11.4.1. keliančius mažą pinigų plovimo ir (ar) teroristų finansavimo grėsmę, jei surinko ne daugiau kaip 1 balą; 11.4.2. keliančius vidutinę pinigų plovimo ir (ar) teroristų finansavimo grėsmę; jei surinko nuo 2 iki 3 balų; 11.4.3. keliančius didelę pinigų plovimo ir (ar) teroristų finansavimo grėsmę, jei surinko 4 ar daugiau balų. 11.5. Kriterijai, kuriais vadovaujantis (atitikus bent vieną kriterijų) laikoma, kad Klientas kelia didelę pinigų plovimo ir (ar) teroristų finansavimo grėsmę: 11.5.1. klientas tapatybės nustatymo momentu vengia atlikti veiksmus, būtinus jo tapatybei nustatyti, ir suteikti informacijos apie save, savo verslą; 11.5.2. klientas Bendrovės prašymu nepateikia dokumentų, patvirtinančių finansinę veiklą; 11.5.3. kliento, kliento atstovo (jeigu piniginė operacija atliekama per atstovą) tapatybę nustatantys duomenys atitinka Lietuvos Respublikos ir tarptautinių organizacijų (FATF, Jungtinių Tautų Organizacijos, Europos Sąjungos) sudarytuose sąrašuose pateiktus su pinigų plovimu ir (ar) teroristine veikla susijusių asmenų duomenis arba jiems taikomos finansinės sankcijos pagal Lietuvos Respublikos ekonominių ir kitų tarptautinių sankcijų įgyvendinimo įstatymą; 11.5.4. Bendrovė nustato, kad atsirado įprastai kliento veiklai nebūdingų požymių (atliekamos piniginės operacijos stambesnėmis sumomis,		11.4. Based on the total number of points obtained, the Customer shall be assigned to one of the following risk categories: 11.4.1. Low money laundering and/or terrorist financing risk, where the Customer scores no more than one (1) point; 11.4.2. Medium money laundering and/or terrorist financing risk, where the Customer scores from two (2) to three (3) points; 11.4.3. High money laundering and/or terrorist financing risk, where the Customer scores four (4) or more points. 11.5. A Customer shall be deemed to present a high money laundering and/or terrorist financing risk if at least one of the following criteria is met: 11.5.1. at the time of the Customer Due Diligence process, the Customer avoids taking the actions necessary for identification or refuses to provide information about themselves or their business; 11.5.2. the Customer fails to provide, upon the Company's request, documents evidencing its financial activities; 11.5.3. the identification data of the Customer or the Customer's representative (where the monetary transaction is carried out through a representative) match the data of persons included in the lists of persons associated with money laundering and/or terrorist activities maintained by the Republic of Lithuania or international organisations (including the FATF, the United Nations and the European Union), or such persons are subject to financial sanctions under the Law on the Implementation of Economic and Other International Sanctions of the Republic of Lithuania; 11.5.4. the Company determines that the Customer has exhibited unusual behaviour inconsistent with the Customer's normal business	

klientas dažnai sudaro naujas paskolos sutartis ir praėjus trumpam laiko tarpui jas padengia ir kita); 12. INFORMACIJOS SAUGOJIMAS IR APSAUGA 12.1. Bendrovė privalo tvarkyti įtartinų piniginių operacijų ar sandorių ir pranešimų apie juos FNTT išsiuntimo registracijos žurnalą (priedas Nr. 1). Duomenys į registracijos žurnalą įrašomi chronologine tvarka, remiantis pinigine operaciją ar sandorį patvirtinančiais dokumentais, sandorių sudarymą patvirtinančiomis sutartimis arba kitais juridinę galią turinčiais dokumentais, susijusiais su piniginių operacijų atlikimu ir/ar sandorių sudarymu, nedelsiant, bet ne vėliau kaip per 3 darbo dienas nuo piniginės operacijos atlikimo ar sandorio sudarymo. 12.2. Bendrovė privalo tvarkyti klientų, su kuriais sandoriai ar dalykiniai santykiai buvo nutraukti Politikos 3.8. punkte nurodytomis aplinkybėmis ar kitomis su pinigų plovimo ir (ar) teroristų finansavimo prevencijos tvarkos pažeidimais susijusiomis aplinkybėmis, registracijos žurnalą (priedas Nr. 2). Duomenys į registracijos žurnalą įrašomi chronologine tvarka ne vėliau kaip per 3 darbo dienas nuo nurodytų aplinkybių atsiradimo ar paaiškėjimo. 12.3. Registracijos žurnalų duomenys saugomi 8 metus nuo sandorių ar dalykinių santykių su klientu pabaigos dienos. 12.4. Kliento tapatybę patvirtinančių dokumentų kopijos, naudos gavėjo tapatybės duomenys, kiti duomenys, gauti kliento tapatybės nustatymo metu, sąskaitų ir (ar) sutarčių dokumentai (dokumentų originalai arba elektroninės formos dokumentai, ataskaitos išsaugoti elektronine forma vadovaujantis Popierinių dokumentų atrankos ir jų išsaugojimo elektronine forma tvarkos aprašu) turi būti saugomi 8 metus nuo	activities (for example, conducting transactions involving unusually large amounts, frequently entering into new loan agreements and repaying them shortly thereafter, or similar activities). 12. RECORD RETENTION AND PROTECTION OF INFORMATION 12.1. The Company shall maintain a register of suspicious monetary transactions or transactions and reports submitted to the Financial Crime Investigation Service (FCIS) (Annex No. 1). Entries shall be made in chronological order on the basis of documents confirming the monetary transaction or transaction, agreements confirming the conclusion of transactions, or other legally valid documents relating to the execution of monetary transactions and/or conclusion of transactions, immediately, but no later than three (3) business days after the execution of the monetary transaction or conclusion of the transaction. 12.2. The Company shall maintain a register of Customers whose transactions or business relationships have been terminated under the circumstances specified in Clause 3.8 of this Policy or due to other breaches of anti-money laundering and counter-terrorist financing requirements (Annex No. 2). Entries shall be made in chronological order no later than three (3) business days after such circumstances arise or become known. 12.3. The data contained in the registers shall be retained for eight (8) years from the date of termination of the transaction or business relationship with the Customer. 12.4. Copies of documents evidencing the Customer's identity, Beneficial Owner identification data, other information obtained during the Customer Due Diligence process, account and/or contractual documents (originals or electronic documents, including reports preserved electronically in accordance with the Procedure for the Selection of Paper Documents and Their Preservation in Electronic
--	--



sandorių ar dalykinių santykių su klientu pabaigos dienos. 12.5. Dalykinių santykių su klientu korespondencija turi būti saugoma 5 metus nuo sandorių ar dalykinių santykių su klientu pabaigos dienos popierinėje arba elektroninėje laikmenoje. 12.6. Saugojimo terminai gali būti papildomai pratęsti ne ilgiau kaip 2 metams, kai yra motyvuotas kompetentingos institucijos nurodymas. 12.7. Piniginę operaciją ar sandorį patvirtinantys dokumentai ar kiti juridinę galią turintys dokumentai, susiję su piniginių operacijų atlikimu ar sandorių sudarymu, turi būti saugomi 8 metus nuo piniginės operacijos atlikimo ar sandorio sudarymo dienos. 12.8. Darbuotojams draudžiama pranešti klientui ar kitiems asmenims, kad informacija apie kliento atliekamas pinigines operacijas arba sudaromus sandorius, arba dėl jų atliekamą tyrimą pateikta FNTT. 13. ATSAKINGO ASMENS FUNKCIJOS IR ATSAKOMYBĖS 13.1. Bendrovės vadovas savo sprendimu paskiria už pinigų plovimo ir terorizmo prevenciją Atsakingą asmenį, kuris vykdo Politikoje numatytas pinigų plovimo ir (ar) terorizmo finansavimo prevencijos priemones. Tuo atveju jeigu Bendrovės vadovas nepaskiria Atsakingo asmens arba Atsakingas asmuo negali vykdyti savo funkcijų, laikoma, kad Atsakingas asmuo yra Bendrovės vadovas. 13.2. Atsakingo asmens funkcijos apima: 13.2.1. žurnalų tvarkymą ir duomenų saugumo	Form) shall be retained for eight (8) years from the date of termination of the transaction or business relationship with the Customer. 12.5. Correspondence relating to the Customer's business relationship shall be retained for five (5) years from the date of termination of the transaction or business relationship with the Customer, either in paper or electronic form. 12.6. The above retention periods may be extended for an additional period of up to two (2) years upon a reasoned instruction from a competent authority. 12.7. Documents evidencing monetary transactions or transactions, or other legally valid documents relating to the execution of monetary transactions or conclusion of transactions, shall be retained for eight (8) years from the date on which the monetary transaction was executed or the transaction concluded. 12.8. Employees are prohibited from informing the Customer or any other person that information concerning the Customer's monetary transactions, transactions entered into by the Customer, or any investigation relating thereto has been reported to the Financial Crime Investigation Service (FCIS). 13. FUNCTIONS AND RESPONSIBILITIES OF THE AML/CFT COMPLIANCE OFFICER 13.1. By its decision, the Company's Director shall appoint an AML/CFT Compliance Officer responsible for the prevention of money laundering and terrorist financing, who shall implement the anti-money laundering and counter-terrorist financing measures set out in this Policy. Where the Company's Director does not appoint an AML/CFT Compliance Officer or where the appointed AML/CFT Compliance Officer is unable to perform his or her duties, the Company's Director shall be deemed to act as the AML/CFT Compliance Officer. 13.2. The functions of the AML/CFT Compliance Officer shall include: 13.2.1. maintaining the required registers and
---	---

užtikrinimą; 13.2.2. Bendrovės visos veiklos Pinigų plovimo ir teroristų finansavimo prevencijos politikos rizikos vertinimą ir valdymą; 13.2.3. įtartinų Piniginių operacijų sustabdymą; 13.2.4. pinigų plovimo ir teroristų finansavimo priemonių prevencijos įgyvendinimą, peržiūrą ir atnaujinimą; 13.2.5. bendradarbiavimą ir komunikaciją su FNTT ir kitomis priežiūros institucijomis su pinigų plovimo ir (ar) teroristų finansavimo prevencija susijusiais klausimais; 13.2.6. Bendrovės darbuotojų supažindinimą su šia Politika; 13.2.7. periodinių mokymų apie pinigų plovimo ir (ar) teroristų finansavimo prevenciją organizavimą Bendrovės darbuotojams. 13.3. Prieš paskirdamas Atsakingą asmenį Bendrovės vadovas įvertina jo kompetenciją, darbo patirtį ir kvalifikaciją pinigų plovimo ir terorizmo finansavimo srityje, išsilavinimo lygį ir pobūdį, kvalifikacijos tobulinimą, profesinės veiklos ar darbo patirties pobūdį ir trukmę, kitus veiksnius, kurie gali turėti įtakos asmens kompetencijai. Bendrovės vadovas užtikrina Atsakingo asmens tinkamą vykdomų funkcijų atskyrimą, kad būtų išvengta interesų konfliktų, dėl kurių padidėja arba gali padidėti pinigų plovimo ir teroristų finansavimo rizika. 13.4. Paskyrus Atsakingą asmenį Bendrovė nedelsiant, tačiau ne vėliau kaip per 7 darbo dienas, apie tokio asmens paskyrimą informuoja FNTT. 13.5. Atsakingas asmuo turi teisę gauti ir susipažinti su visa informacija reikalinga jo funkcijoms vykdyti, įskaitant prieigą prie visos informacijos susijusios su klientais, jų atstovais, naudos gavėjais ir prie informacijos apie visas	ensuring the security of the data contained therein; 13.2.2. assessing and managing money laundering and terrorist financing risks across the Company's entire business; 13.2.3. suspending suspicious monetary transactions; 13.2.4. implementing, reviewing and updating the Company's anti-money laundering and counter-terrorist financing measures; 13.2.5. cooperating and communicating with the Financial Crime Investigation Service (FCIS) and other supervisory authorities on matters relating to the prevention of money laundering and terrorist financing; 13.2.6. ensuring that the Company's Employees are familiarised with this Policy; 13.2.7. organising periodic anti-money laundering and counter-terrorist financing training for the Company's Employees. 13.3. Before appointing an AML/CFT Compliance Officer, the Company's Director shall assess that person's competence, professional experience and qualifications in the field of anti-money laundering and counter-terrorist financing, educational background, continuing professional development, the nature and duration of professional or work experience, and any other factors that may affect the person's competence. The Company's Director shall ensure an appropriate segregation of duties for the AML/CFT Compliance Officer in order to prevent conflicts of interest that increase or may increase money laundering and terrorist financing risks. 13.4. Following the appointment of the AML/CFT Compliance Officer, the Company shall notify the Financial Crime Investigation Service (FCIS) thereof without undue delay, but no later than seven (7) business days after the appointment. 13.5. The AML/CFT Compliance Officer shall have the right to obtain and review all information necessary for the performance of his or her duties, including unrestricted access to information relating to Customers, their
--	--

Bendrovės ir Bendrovės klientų vykdomas Pinigines operacijas. 13.6. Atsakingas asmuo užtikrina, kad gavus FNTT užklausą, jų prašoma informacija būtų pateikiama nedelsiant, tačiau ne vėliau kaip per 14 darbo dienų nuo paklausimo gavimo (tais atvejais kai PPTFPJ nustatyti trumpesni informacijos pateikimo FNTT terminai, tokia informacija turi būti pateikiama per trumpesnius terminus). 13.7. Atsakingas asmuo užtikrins, kad Politika ir kitos Bendrovės pinigų prevencijos ir terorizmo finansavimo prevencijos priemonės būtų peržiūrimos bent kartą metuose ir esant poreikiui atnaujinamos. 13.8. Atsakingas asmuo Bendrovės vadovui periodiškai, tačiau ne rečiau kaip kartą į metus pateikia pinigų plovimo ir terorizmo finansavimo priemonių įgyvendinimo ataskaitą, kurioje pateikia informaciją bent apie: 13.8.1. Pinigų plovimo ir teroristų finansavimo rizikos valdymą, kuri apima: 13.8.1.1. Bendrovės patiriamą pinigų plovimo ir teroristų finansavimo riziką ir jos lygio pasikeitimus; 13.8.1.2. įdiegtas pinigų plovimo ir teroristų finansavimo rizikos valdymo priemones; 13.8.1.3. pasiūlymus dėl priemonių, reikalingų pinigų plovimo ir teroristų finansavimo rizikai veiksmingai valdyti (mažinti), pakeitimo; 13.8.1.4. informaciją apie pažeidimus, nustatytus įgyvendinant vidaus kontrolės procedūras ir politikas pinigų plovimo ir teroristų finansavimo prevencijos srityje; 13.8.1.5. atsiskaitymą, kaip Bendrovė vykdo reikalavimus ir pareigas, susijusias su pinigų plovimo ir teroristų finansavimo prevencija.	representatives, Beneficial Owners, and all monetary transactions carried out by the Company and its Customers. 13.6. The AML/CFT Compliance Officer shall ensure that any request for information received from the FCIS is answered without undue delay and, in any event, no later than fourteen (14) business days after receipt of the request (provided that, where the AML/CFT Law prescribes shorter deadlines for providing information to the FCIS, such shorter deadlines shall apply). 13.7. The AML/CFT Compliance Officer shall ensure that this Policy and all other anti-money laundering and counter-terrorist financing measures implemented by the Company are reviewed at least once a year and updated whenever necessary. 13.8. The AML/CFT Compliance Officer shall submit to the Company's Director, on a periodic basis and at least once a year, a report on the implementation of anti-money laundering and counter-terrorist financing measures, including at least the following information: 13.8.1. information on money laundering and terrorist financing risk management, including: 13.8.1.1. the money laundering and terrorist financing risks faced by the Company and any changes in their level; 13.8.1.2. the money laundering and terrorist financing risk management measures implemented by the Company; 13.8.1.3. proposals for amendments to measures necessary for the effective management and mitigation of money laundering and terrorist financing risks; 13.8.1.4. information on deficiencies or breaches identified in the implementation of internal control procedures and policies relating to anti-money laundering and counter-terrorist financing; 13.8.1.5. a report on the Company's compliance with its obligations and regulatory requirements relating to anti-money laundering and counter-
--	--

13.9. Bendrovės darbuotojams kilus įtarimams, kad Piniginė operacija gali būti įtartina arba atradus kitų galimų pinigų plovimo ir (ar) terorizmo finansavimo požymių, jie privalo nedelsiant apie tai informuoti Atsakingą asmenį. 14. TAPATYBĖS NUSTATYMO IR STEBĖSENOS VEIKLOS FUNKCIJŲ PERDAVIMAS KITAM ASMENIUI 14.1. Bendrovė turi teisę perduoti kliento ir naudos gavėjo tapatybės nustatymo ir nuolatinės dalykinių santykių stebėsenos veiklos funkcijas (toliau – veiklos funkcijos) kitam Europos Sąjungos valstybėje narėje arba trečiojoje valstybėje, kuri taiko Europos Sąjungos valstybėje narėje nustatytiems klientų ir naudos gavėjų tapatybės nustatymo reikalavimams ir informacijos saugojimo reikalavimams lygiaverčius reikalavimus, registruotam asmeniui, kuris nėra trečioji šalis (toliau šiame straipsnyje – kitas asmuo). 14.2. Bendrovė perduodama Politikos 14.1. punkte nurodytas veiklos funkcijas kitam asmeniui, turi laikytis šių reikalavimų: 14.2.1. tarp Bendrovės ir kito asmens, kuriam yra perduodamos veiklos funkcijos, yra sudaryta rašytinė sutartis, nustatanti, be kita ko, veiklos funkcijų perdavimą, reguliary kliento ir naudos gavėjo tapatybės nustatymo metu pateiktų dokumentų, duomenų ar informacijos atnaujinimą, keitimąsi informacija apie nustatytus šiame įstatyme nurodytų kliento ir naudos gavėjo tapatybės nustatymo reikalavimų pažeidimus; 14.2.2. prieš perduodama veiklos funkcijas kitam asmeniui, Bendrovė įsitikino, kad kitas asmuo laikosi PPTFPĮ nurodytų kliento ar naudos gavėjo tapatybės nustatymo reikalavimų. Paaškęjus naujoms aplinkybėms ar pasikeitus teisės normoms, Bendrovė privalo peržiūrėti ir atnaujinti informaciją, ar kitas asmuo laikosi PPTFPĮ nurodytų kliento ar naudos gavėjo tapatybės nustatymo reikalavimų, ir tęsti veiklos funkcijų perdavimą tik	terrorist financing. 13.9. Where Company Employees suspect that a monetary transaction may be suspicious or identify any other indicators of possible money laundering and/or terrorist financing, they shall immediately notify the AML/CFT Compliance Officer. 14. OUTSOURCING OF CUSTOMER DUE DILIGENCE AND ONGOING MONITORING FUNCTIONS 14.1. The Company may outsource Customer and Beneficial Owner identification and ongoing business relationship monitoring functions (hereinafter, the "Outsourced Functions") to another person established in a Member State of the European Union or in a third country that applies requirements equivalent to those applicable in the European Union with respect to Customer and Beneficial Owner identification and record retention, provided that such person is not a Third Party within the meaning of this Policy (hereinafter, the "Service Provider"). 14.2. When outsourcing the functions referred to in Clause 14.1, the Company shall comply with the following requirements: 14.2.1. the Company and the Service Provider shall enter into a written agreement governing, inter alia, the outsourcing of the relevant functions, the regular updating of documents, data and information collected during Customer and Beneficial Owner identification, and the exchange of information regarding any breaches of the Customer and Beneficial Owner identification requirements established under the AML/CFT Law; 14.2.2. before outsourcing the relevant functions, the Company shall verify that the Service Provider complies with the Customer and Beneficial Owner identification requirements established by the AML/CFT Law. Where new circumstances arise or legal requirements change, the Company shall review and update its assessment of the Service Provider's compliance and may continue outsourcing such
--	---

tuo atveju, jeigu įsitikino, kad kitas asmuo laikosi PPTFPĮ nurodytų kliento ar naudos gavėjo tapatybės nustatymo reikalavimų. Bendrovė privalo PPTFPĮ numatytų patikrinimų rezultatus įforminti raštu; 14.2.3. kitam asmeniui negali būti perduodamas kliento įtartinų piniginių operacijų ar sandorių nustatymas ir pranešimų apie tai teikimas, taip pat Politikos 12 skyriuje nurodytos informacijos saugojimas; 14.2.4. Bendrovė užtikrina, kad asmens duomenys tvarkomi laikantis PPTFPĮ 24 straipsnyje nustatytų reikalavimų. 14.3. Atsakomybė dėl šiame Politikos skyriuje nurodytų kliento ir naudos gavėjo tapatybės nustatymo ir nuolatinės dalykinių santykių stebėsenos reikalavimų laikymosi tenka Bendrovei. 15. BAIGIAMOSIOS NUOSTATOS 15.1. Darbuotojai, pažeidę Politikos ir Politikos 1.2 punkte nurodytų teisės aktų reikalavimus, atsako įstatymų nustatyta tvarka. 15.2. Su Politika turi būti supažindinti ir jomis privalo vadovautis visi Bendrovės darbuotojai, kuriems jos gali būti aktualios. 15.3. Šią Politiką tvirtina Bendrovės vadovas. Ši Politika gali būti panaikinta, keičiama ar papildoma tik Bendrovės direktoriaus sprendimu. Politika ar jos pakeitimai įsigalioja Bendrovės direktoriaus sprendimo priėmimo dieną, išskyrus tuos atvejus kai direktoriaus sprendime numatoma kita įsigaliojimo data. 16. PRIEDAI 16.1. Priedas Nr. 1 – Įtartinų piniginių operacijų ar sandorių ir pranešimų apie juos FNTT išsiuntimo registracijos žurnalas. 16.2. Priedas Nr. 2 – Klientų, su kuriais sandoriai ar dalykiniai santykiai nutraukti Politikos 3.7. punkte nurodytomis aplinkybėmis ar kitomis su pinigų	functions only after confirming that the Service Provider remains compliant with the applicable AML/CFT requirements. The Company shall document the results of such assessments in writing; 14.2.3. the identification of suspicious monetary transactions or transactions and the reporting thereof, as well as the storage of information referred to in Section 12 of this Policy, may not be outsourced to the Service Provider; 14.2.4. the Company shall ensure that personal data are processed in accordance with the requirements of Article 24 of the AML/CFT Law. 14.3. The Company shall remain fully responsible for compliance with all Customer and Beneficial Owner identification and ongoing business relationship monitoring requirements referred to in this Section of the Policy. 15. FINAL PROVISIONS 15.1. Employees who breach the requirements of this Policy or the legal acts referred to in Clause 1.2 of this Policy shall be liable in accordance with applicable law. 15.2. All Company Employees to whom this Policy may be relevant shall be familiarised with its provisions and shall comply with them. 15.3. This Policy shall be approved by the Company's Director. This Policy may be revoked, amended or supplemented only by a decision of the Company's Director. The Policy and any amendments thereto shall enter into force on the date of the Director's decision approving them, unless another effective date is specified in such decision. 16. ANNEXES 16.1. Annex No. 1 – Register of Suspicious Monetary Transactions or Transactions and Reports Submitted to the Financial Crime Investigation Service (FCIS). 16.2. Annex No. 2 – Register of Customers Whose Transactions or Business Relationships Have Been Terminated under the Circumstances Referred to
---	---



plovimo ir (ar) teroristų finansavimo prevencijos tvarkos pažeidimais susijusiomis aplinkybėmis, registracijos žurnalas. 16.3. Priedas Nr. 3 – Kliento anketa.	in Clause 3.7 of this Policy or Due to Other Breaches of Anti-Money Laundering and Counter-Terrorist Financing Requirements. 16.3. Annex No. 3 – Customer Questionnaire.
---	---