ЗАТВЕРДЖЕНО
РІШЕННЯМ ЄДИНОГО УЧАСНИКА
ТОВ «АЛЕКСКРЕДИТ»
№ 20/03-24 від 20 березня 2024 р.

Директор_____ Анатолій ПОПУДРЕНКО

ПОЛОЖЕННЯ

про використання електронного підпису та електронної печатки

ТОВАРИСТВА З ОБМЕЖЕНОЮ ВІДПОВІДАЛЬНІСТЮ «АЛЕКСКРЕДИТ»

м. Дніпро
2024 рік

ЗМІСТ

6. ЗАКЛЮЧНІ ПОЛОЖЕННЯ.

1. ЗАГАЛЬНІ ПОЛОЖЕННЯ

Це Положення про використання електронного підпису та електронної печатки (далі по тексту-Положення) є внутрішнім нормативним документом ТОВ «АЛЕКСКРЕДИТ» (далі - Товариство) та визначає порядок застосування електронного підпису та електронної печатки під час створення, приймання, реєстрації, оброблення, зберігання та надсилання електронних документів в інформаційних системах та сервісах Товариства та встановлює вимоги щодо надання, скасування та контролю доступу до інформаційних систем установи, що використовуються для приймання, реєстрації, оброблення, зберігання, надсилання електронних документів.

Положення розроблено відповідно до вимог Законів України «Про електронну ідентифікацію та електронні довірчі послуги», «Про електронні документи та електронний документообіг», Закону України «Про електронну комерцію», Закону України «Про захист інформації в інформаційно-комунікаційних системах», Закону України «Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення», Постанови Кабінету Міністрів України «Про затвердження вимог до форматів удосконалених електронних підписів та печаток, які використовуються для надання електронних публічних послуг, та вимог до створення та перевірки удосконалених електронних підписів та печаток, що базуються на кваліфікованих сертифікатах відкритих ключів» від 12.12.2023 № 1298, Положення про здійснення установами фінансового моніторингу від 28.07.2020 № 107, «Положення про використання електронного підпису та електронної печатки», затвердженого Постановою Правління Національного банку України № 172 від 20.12.2023.

Положення розроблено з метою забезпечення захисту цілісності інформації, гарантування достовірності переданої та отриманої інформації, а також виявлення будь-яких змін в електронному документі при використанні електронного підпису у Товаристві.

Товариство надає можливість безперешкодного ознайомлення з цим Положенням всім учасникам (суб'єктам) електронного документообігу, які використовують електронний підпис, в тому числі клієнтам та потенційним клієнтам Товариства.

2. ТЕРМІНИ ТА СКОРОЧЕННЯ

У Положенні використовуються такі терміни:

Автентифікація - електронний процес, що дає змогу підтвердити електронну ідентифікацію фізичної, юридичної особи, інформаційної або інформаційно-комунікаційної системи та/або походження та цілісність електронних даних.

Авторизація - керування рівнями та засобами доступу до певного

захищеного ресурсу, являється частиною процедури надання доступу для роботи в інформаційній системі, після ідентифікації і автентифікації.

Верифікація - заходи, що вживаються суб'єктом первинного фінансового моніторингу з метою перевірки (підтвердження) належності відповідній особі отриманих суб'єктом первинного фінансового моніторингу ідентифікаційних даних та/або з метою підтвердження даних, що дають змогу встановити кінцевих бенефіціарних власників чи їх відсутність.

Відкритий ключ – (дані для підтвердження електронного підпису чи електронної печатки) - дані, що використовуються для підтвердження електронного підпису чи електронної печатки.

Договір — договір про надання кредиту, укладений між Кредитодавцем та Позичальником виключно в письмовій формі у вигляді електронного документа, підписаний Позичальником шляхом використання Електронного підпису одноразовим ідентифікатором, а Кредитодавцем – шляхом використання факсимільного відтворення аналога підпису уповноваженої особи та відбитку печатки Кредитодавця.

Електронний документ - документ, інформація в якому зафіксована у вигляді електронних даних, включаючи обов'язкові реквізити документа.

Електронний підпис (ЕП) - електронні дані, що додаються до інших електронних даних або логічно з ними пов'язуються і використовуються підписувачем як підпис.

Електронний підпис одноразовим ідентифікатором – дані в електронній формі у вигляді алфавітно-цифрової послідовності, що додаються до інших електронних даних Заявником/Позичальником, який прийняв пропозицію (Оферту) Кредитодавця укласти Договір/внести зміни до Договору, та надсилаються ним Кредитодавцю.

Електронна ідентифікація - процес використання ідентифікаційних даних особи в електронній формі, які однозначно визначають фізичну, юридичну особу або уповноваженого представника юридичної особи.

Електронна печатка - електронні дані, що додаються до інших електронних даних або логічно з ними пов'язуються і використовуються для забезпечення достовірності походження пов'язаних електронних даних, або для засвідчення електронних підписів підписувачів на електронних документах, або для засвідчення відповідності копій документів оригіналам та виявлення порушення цілісності.

Електронна позначка часу - електронні дані, що пов'язують інші електронні дані з конкретним моментом часу для засвідчення наявності цих електронних даних на цей момент часу.

Ідентифікація - заходи, що вживаються суб'єктом первинного фінансового моніторингу для встановлення особи шляхом отримання її ідентифікаційних даних.

Ідентифікація особи - процес використання ідентифікаційних даних особи з документів, створених на матеріальних носіях, та/або електронних даних, у результаті якого забезпечується однозначне встановлення фізичної, юридичної особи або уповноваженого представника юридичної особи та

перевірка належності особі таких даних.

Інформаційна (автоматизована) система - організаційно-технічна система, в якій реалізується технологія обробки інформації з використанням технічних і програмних засобів.

Кваліфікована електронна печатка - удосконалена електронна печатка, що створюється з використанням засобу кваліфікованої електронної печатки і базується на кваліфікованому сертифікаті електронної печатки.

Кваліфікована електронна позначка часу — електронна позначка часу, яка пов'язує дату і час з електронними даними в такий спосіб, що обґрунтовано виключає можливість зміни електронних даних, яка не може бути виявлена; базуватися на джерелі точного часу, синхронізованому із Всесвітнім координованим часом (UTC) з точністю до секунди; до якої додається створений для неї удосконалений електронний підпис чи удосконалена електронна печатка кваліфікованого надавача електронних довірчих послуг або може застосовувати інший метод, рівнозначний додаванню до кваліфікованої електронної позначки часу удосконаленого електронного підпису чи удосконаленої електронної печатки, за умови що він забезпечує рівнозначний рівень безпеки кваліфікованої електронної позначки часу.

Кваліфікований електронний підпис (КЕП) - удосконалений електронний підпис, що створюється з використанням засобу кваліфікованого електронного підпису і базується на кваліфікованому сертифікаті електронного підпису.

Клієнт — фізична особа, яка уклала або має намір укласти з Кредитодавцем договір про надання кредиту.

Контрагент установи - будь-яка юридична чи фізична особа, фізична особа-підприємець, фізична особа, яка провадить незалежну професійну діяльність, яка має з Товариством відносини фінансового характеру. Контрагент може одночасно мати з Товариством трудові відносини або відносини іншого характеру.

Логін - унікальна комбінація букв та/або цифр, що встановлюється Заявником/Позичальником. Цю комбінацію Заявник/Позичальник самостійно зазначає в спеціальному полі «Логін» при вході до Особистого кабінету.

Особистий ключ - (дані для створення електронного підпису чи печатки) - унікальні дані, що використовуються підписувачем чи створювачем електронної печатки для створення електронного підпису чи печатки.

Особистий кабінет - частина Сайту Кредитодавця. Доступ до Особистого кабінету здійснюється Заявником/Позичальником після авторизації, яка проходить шляхом введення Логіна і Пароля від Особистого кабінету.

Пароль – унікальна комбінація букв та/або цифр, що встановлюється Заявником/Позичальником при вході до Особистого кабінету.

Підписувач — фізична особа, яка створює електронний підпис.

Позичальник – фізична особа, яка уклала Договір з Кредитодавцем.

Підтвердження електронного підпису чи печатки - процес перевірки та підтвердження дійсності електронного підпису чи печатки.

Підтвердження електронної ідентифікації - процес перевірки та підтвердження належності ідентифікаційних даних фізичній, юридичній особі або уповноваженому представнику юридичної особи.

Перевірка цілісності - процедура, яка дає змогу виявити будь-які зміни в електронному документі та зміни ЕП після підписання електронного документа.

Простий електронний підпис (Простий ЕП) - будь-який вид ЕП, крім кваліфікованого ЕП, цифрового власноручного підпису (далі - ЦВП), УЕП з кваліфікованим сертифікатом, УЕП, ЕП Національного банку.

Сертифікат відкритого ключа - електронний документ, який засвідчує належність відкритого ключа фізичній або юридичній особі, підтверджує її ідентифікаційні дані та/або надає можливість здійснити автентифікацію веб-сайту.

Сертифікат електронного підпису - електронне свідоцтво, що пов'язує відкритий ключ електронного підпису з фізичною особою та підтверджує щонайменше прізвище, власне ім'я, по батькові (за наявності) або псевдонімізацію такої особи.

Сертифікат електронної печатки - електронне свідоцтво, що пов'язує відкритий ключ електронної печатки з юридичною особою, особою, яка здійснює господарську діяльність, та підтверджує найменування такої особи.

Удосконалена електронна печатка - електронна печатка, яка однозначно пов'язана з підписувачем або її створювачем печатки; надає можливість ідентифікувати підписувача або її створювача; створюється з використанням особистого ключа, який підписувач або її створювач може з високим рівнем достовірності використовувати під власним одноосібним контролем; пов'язана з електронними даними, на які накладено удосконалений електронний підпис чи печатку, таким чином, щоб будь-яка наступна зміна таких даних могла бути виявлена.

Інші терміни, які вживаються у Положенні, застосовуються у значеннях, наведених у законодавстві України, яке регламентує питання захисту інформації.

3. ПОРЯДОК ВИКОРИСТАННЯ ЕЛЕКТРОННОГО ПІДПИСУ (ЕП)

3.1. Вимоги до ЕП

ЕП є обов'язковим реквізитом електронного документа.

Клієнт, що підписав електронний документ ЕП, у такий спосіб засвідчує, що ознайомився з усім текстом документа, повністю зрозумів його зміст, та не має заперечень до тексту документа.

ЕП які застосовуються у Товаристві мають юридичну силу незалежно від технологій, що застосовуються для створення ЕП, та відповідають наступним вимогам:

- електронні дані, що використовуються для створення ЕП, є унікальними та однозначно пов’язані із Підписувачем і не пов’язані з жодною іншою особою;
- ЕП дає змогу однозначно ідентифікувати Підписувача;
- технологія застосування ЕП забезпечує Підписувачу під час підписання контроль електронних даних, які підписуються, та електронних даних, які використовуються для створення ЕП;
- під час перевірки, здійсненої відповідно до вимог цього Положення, не виявлено будь-яких змін в електронному документі;
- під час перевірки, здійсненої відповідно до вимог цього Положення, не виявлено будь-яких змін ЕП після підписання електронного документа.

3.2. Види електронного підпису, які використовуються у Товаристві під час створення, оброблення та зберігання електронних документів

У Товаристві під час створення, оброблення та зберігання електронних документів використовуються:

- ***Кваліфікований електронний підпис (КЕП).***
- ***Удосконалений електронний підпис (УЕП).***
- ***Аналог власноручного підпису*** (факсимільне відтворення підпису за допомогою засобів механічного або іншого копіювання, іншого аналога власноручного підпису).

3.3. Порядок створення і засвідчення електронної копії з паперового документа

Електронна копія оригіналу паперового документа (фотокопія) - візуальне подання паперового документа в електронній формі, отримане шляхом сканування (фотографування) паперового документа, відповідність оригіналу та правовий статус якого засвідчено кваліфікованою електронною печаткою Товариства.

Електронна копія оригіналу документа в паперовій формі створюється працівником Товариства шляхом сканування (фотографування) виключно з оригіналу документа на паперовому носії інформації.

Електронна копія оригіналу паперового документа засвідчується накладанням електронного підпису та/або електронної печатки. Електронна копія без електронного підпису прирівнюється за статусом незавіреній електронній копії оригіналу документа на паперовому носії інформації.

З метою засвідчення електронної копії паперового документа в Товаристві застосовується ЕП, який застосовується шляхом його накладання на електронну копію документа. Для зазначення на електронних документах часу їх підписання використовуються метадані ЕП.

Для засвідчення підпису на документах та відповідності копій документів оригіналам, Товариство застосовує електронну печатку.

Юридична сила електронного документа не може бути заперечена

виключно через те, що він має електронну форму.

3.4. Порядок створення і засвідчення паперової копії електронного документа

Оригіналом електронного документа вважається електронний примірник документа з обов'язковими реквізитами, у тому числі з електронним підписом автора або підписом, прирівняним до власноручного підпису відповідно до Закону України «Про електронну ідентифікацію та електронні довірчі послуги».

Копією документа на папері для електронного документа є візуальне подання електронного документа на папері, яке засвідчене в порядку, встановленому законодавством.

Оригінал електронного документа повинен давати змогу довести його цілісність та справжність у порядку, визначеному законодавством; у визначених законодавством випадках може бути пред'явлений у візуальній формі відображення, в тому числі у паперовій копії.

У разі створення паперової копії з електронного документу працівник Товариства, який створює таку копію, спочатку проводить обов'язкову перевірку цілісності електронного документу засобами перевірки ЕП, вбудованих в програмні комплекси (WEB-сервіси в мережі Інтернет) електронного документообігу, або WEB-сервіси в мережі Інтернет на офіційному сайті кваліфікованого надавача електронних довірчих послуг.

Після перевірки цілісності працівник Товариства може створити паперові копії з електронного документа шляхом його роздрукування на папері разом з усіма обов'язковими для цього документа реквізитами та засвідчення паперової копії у відповідності до вимог внутрішніх нормативних документів Товариства.

Копія документа набирає юридичної сили лише в разі її засвідчення в порядку, установленому законодавством України. Напис про засвідчення копії в паперовій формі складається зі слів «Згідно з оригіналом», найменування посади, особистого підпису особи, яка засвідчує копію, її власного імені та прізвища, дати засвідчення копії та проставляється нижче реквізиту документа «Підпис». На лицьовому боці у верхньому правому куті першого аркуша документа проставляється відповідна відмітка «Копія», а також, що даний документ є копією з електронного документа. Сторінки копії документів (за винятком тих, що мають один аркуш) нумеруються і відмітка про засвідчення копії доповнюється відміткою «Усього в копії__арк.». Допускається засвідчувати копії документів поаркушно.

Не допускається виготовляти копії документів з нерозбірливим текстом, підчистками, приписами та іншими необумовленими виправленнями.

Товариство зобов'язане після створення електронного документа надати на належним чином оформлену вимогу клієнта / контрагента можливість отримати примірник цього електронного документа з усіма потрібними реквізитами на адресу електронної пошти, зазначену клієнтом / контрагентом або надати електронний документ в інший спосіб, узгоджений із клієнтом /

контрагентом.

В разі здійснення правочину у вигляді електронного документа, Товариство зобов'язане надати клієнту на його вимогу, оформлену згідно вимог, встановлених у Товаристві, засвідчену копію на папері з електронного документа.

Товариство подає документи До Національного банку України з урахуванням вимог «Положення про загальні вимоги до документів і порядок їх подання до Національного банку України в межах окремих процедур та внесення змін до деяких нормативно-правових актів Національного банку України», затвердженого Постановою Правління Національного Банку України від № 200 від 29.12.2023.

Документи до Національного банку України можуть подаватись в один із способів:

- у паперовій формі з одночасним обов’язковим поданням електронних копій цих документів (без накладення КЕП) на цифрових носіях інформації (USB-флешнакопичувачах) або засобами електронного зв’язку, які використовуються Національним банком для електронного документообігу;
- у формі електронного документа та/або електронної копії оригіналу документа в паперовій формі, підписаного шляхом накладання КЕП, - електронним повідомленням на офіційну електронну поштову скриньку Національного банку nbu@bank.gov.ua або іншими засобами електронного зв’язку, які використовуються Національним банком для електронного документообігу.

У разі подання до Національного банку копії документа Товариства (електронної копії паперового документа), така копія документа (електронна копія документа), засвідчується підписом (КЕП для електронних копій документів) уповноваженого представника Товариства.

Електронні документи та електронні копії документів повинні мати коротку назву латинськими літерами, що відображає зміст і реквізити документа.

Електронні копії документів у паперовій формі створюються шляхом сканування з документів у паперовій формі з урахуванням таких вимог:

- документ зберігається у файл формату pdf;
- сканована копія кожного окремого документа зберігається як окремий файл;
- документи, що містять більше однієї сторінки, зберігаються в один файл;
- роздільна здатність сканування повинна бути не нижче ніж 300 dpi.

3.5. Порядок виявлення будь-яких змін в електронному документі, в електронній копії з паперового документа

Перевірка цілісності електронного документа проводиться шляхом підтвердження ЕП чи електронної печатки.

Перевірка цілісності, достовірності та авторства електронних документів здійснюється у Товаристві за допомогою засобів автоматизації та програмно-технічних засобів перевірки чинності.

Для перевірки цілісності електронних документів підписаних КЕП, Товариством використовуються державні онлайн ресурси, які використовують криптографічні алгоритми та протоколи, що відповідають чинному законодавству України.

За наявності будь-яких чинників, що ставлять під сумнів достовірність електронного документа та чинність електронного підпису, яким засвідчувався електронний документ, Товариство відмовляє в його прийманні.

Товариство зберігає електронні документи на електронних носіях інформації у формі, що дає змогу перевірити їх цілісність на цих носіях. Перевірка цілісності електронного документа проводиться шляхом перевірки ЕП підписувача.

Відповідальність за виявлення будь-яких змін в електронних документах покладається на працівників Товариства, які у своїй діяльності та/або процесах створюють, супроводжують електронні документи.

3.6. Порядок виявлення будь-яких змін ЕП після підписання електронного документа

Дотримання порядку виявлення будь-яких змін в електронному підписі після підписання електронного документа має ключове значення для забезпечення безпеки та юридичної вірогідності документів та забезпечує високий рівень їх безпеки.

З метою виявлення будь-яких змін в ЕП після підписання електронного документа Товариством здійснюється:

Захист ключів електронного підпису шляхом застосування паролів, використання апаратного зберігання ключів або інших методів шифрування;

Перевірка цілісності підписаного документа відбувається шляхом перевірки ЕП за допомогою відкритих сервісів в мережі інтернет на офіційних сайтах кваліфікованих надавачів електронних довірчих послуг;

Перевірка дійсності підпису, яка полягає у визначенні, чи був підпис зроблений за допомогою дійсного приватного ключа підписувача. Ця перевірка включає здійснення перевірки метаданих ЕП, терміну дії сертифіката, тощо;

Перевірка електронної позначки часу, яка проводиться за допомогою відкритого ключа, наданого акредитованим центром сертифікації ключів для підтвердження наявності електронного документа на певний момент часу.

У процесі здійснення своєї діяльності Товариством використовуються виключно ті електронні документи, щодо яких проведено належну перевірку цілісності електронного документа.

Відповідальність за виявлення будь-яких змін електронного підпису покладається на працівників Товариства, які у своїй діяльності створюють,

супроводжують та підписують електронні документи.

3.7 . Порядок використання ЕП та електронних печаток Товариства

Порядок використання УЕП та порядок роботи з удосконаленою електронною печаткою

Дотримання порядку роботи з удосконаленою електронною печаткою та допомагають забезпечити її ефективне та безпечне використання в Товаристві.

Товариство застосовує удосконалену електронну печатку в разі вчинення правочинів у вигляді електронних документів або під час здійснення інформаційного обміну з іншими суб'єктами електронної взаємодії на підставі договору з урахуванням вимог «Положення про використання електронного підпису та електронної печатки», затвердженого Постановою Правління Національного банку № 172 від 20.12.2023.

У випадку використання УЕП та засобів удосконаленого електронного підпису чи печатки, що використовуються під час взаємодії Товариства з клієнтом установи, Товариство самостійно визначає технологію використання УЕП та засобів удосконаленого електронного підпису чи печатки.

Товариство має право застосовувати удосконалену електронну печатку для внутрішнього документообігу на підставі розпорядчого акта Товариства.

Удосконалена електронна печатка створюється, якщо відповідно до умов договору потрібно:

- засвідчити дійсність підпису на електронних документах;
- проставити печатку для засвідчення відповідності копій документів оригіналам;
- підтвердити повноваження представника юридичної особи на застосування електронного підпису у контексті, передбаченому документом (підписання, затвердження, погодження, візування, засвідчення, ознайомлення).

УЕП є таким, що пройшов перевірку, якщо виконуються всі такі вимоги:

- перевірку УЕП здійснено згідно з процедурою, зазначеною в договорі, укладеному між суб'єктами електронної взаємодії;
- УЕП відповідає вимогам, визначеним Законом.

Товариство має право використовувати більше ніж одну удосконалену електронну печатку.

Порядок використання КЕП та порядок роботи з кваліфікованою електронною печаткою

Використання КЕП та печаток забезпечує високий рівень довіри до схем електронної ідентифікації.

КЕП має таку саму юридичну силу, як і власноручний підпис, та має презумпцію його відповідності власноручному підпису.

Кваліфікована електронна печатка має презумпцію цілісності

електронних даних і достовірності походження електронних даних, з якими вона пов’язана.

Товариство забезпечує приймання, реєстрацію, підтвердження про отримання електронних документів із створеними КЕП з дотриманням вимог законодавства України у сфері електронного документообігу та функціонування електронної поштової скриньки для приймання, реєстрації, підтвердження про отримання електронних документів із створеними КЕП клієнтів / контрагентів.

Товариство має право застосовувати кваліфіковану електронну печатку в разі надання або отримання послуг в електронній формі або під час здійснення інформаційного обміну з іншими суб'єктами електронної взаємодії.

Кваліфікований сертифікат електронної печатки повинен відповідати вимогам Закону України «Про електронну ідентифікацію та електронні довірчі послуги» та мати позначку, що цей сертифікат сформовано як кваліфікований для використання електронної печатки.

Перевірка та підтвердження кваліфікованої електронної печатки здійснюється відповідно до вимог Закону України «Про електронну ідентифікацію та електронні довірчі послуги».

Товариство має право використовувати більше ніж одну кваліфіковану електронну печатку.

Товариство забезпечує застосування кваліфікованої електронної позначки часу у випадках створення і використання кваліфікованої електронної печатки, якщо:

- відповідно до законодавства України потрібно засвідчити дійсність підпису на електронних документах;
- відповідно до законодавства України проставлення печатки вимагається для засвідчення відповідності копій документів оригіналам;
- потрібно підтвердити повноваження представника юридичної особи на застосування електронного підпису у контексті, передбаченому документом (підписання, затвердження, погодження, візування, засвідчення, ознайомлення);
- в інших випадках, відповідно до вимог чинного законодавства.

Створення кваліфікованої електронної печатки для електронних документів здійснюють працівники Товариства, згідно з повноваженнями, що визначаються розпорядчими документами Товариства.

Товариство не має права подавати один і той самий відкритий ключ кільком кваліфікованим надавачам електронних довірчих послуг для формування кваліфікованого сертифіката відкритого ключа і засвідчення його чинності.

Перед застосуванням КЕП відповідальний працівник Товариства в обов’язковому порядку здійснює його належну перевірку та підтвердження.

Перевірка та підтвердження КЕП здійснюється відповідно до вимог Закону України «Про електронну ідентифікацію та електронні довірчі

послуги». У Товаристві забороняється використання КЕП з нечинним кваліфікованим сертифікатом електронної печатки. Документи, які підписані невалідним на момент підписання КЕП, не визнаються документами Товариства.

Перевірка чинності кваліфікованого сертифіката електронної печатки здійснюється виключно засобом кваліфікованого електронного підпису чи печатки відповідно до вимог Закону України «Про електронну ідентифікацію та електронні довірчі послуги».

КЕП чи печатка вважається таким, що пройшов перевірку та отримав підтвердження, якщо:

- перевірку кваліфікованого електронного підпису чи печатки проведено засобом кваліфікованого електронного підпису, чи печатки;
- перевіркою встановлено, що відповідно до вимог Закону України «Про електронну ідентифікацію та електронні довірчі послуги» на момент створення кваліфікованого електронного підпису чи печатки був чинним кваліфікований сертифікат електронного підпису, чи печатки підписувача, чи створювача електронної печатки;
- за допомогою кваліфікованого сертифіката електронного підпису чи печатки здійснено ідентифікацію підписувача, чи створювача електронної печатки;
- під час перевірки за допомогою кваліфікованого сертифіката електронного підпису чи печатки отримано підтвердження того, що особистий ключ, який належить підписувачу, чи створювачу електронної печатки, зберігається в засобі кваліфікованого електронного підпису, чи печатки;
- під час перевірки підтверджено цілісність електронних даних в електронній формі, з якими пов’язаний цей кваліфікований електронний підпис чи печатка.

Під час створення кваліфікованої електронної печатки відповідальний працівник Товариства здійснює перевірку чинності кваліфікованого сертифіката відкритого ключа.

Кваліфікований сертифікат відкритого ключа вважається чинним у разі, якщо на момент перевірки чинності:

- строк дії, зазначений у кваліфікованому сертифікаті відкритого ключа, не закінчився;
- суб’єктом, який видав сертифікат, статус кваліфікованого сертифіката відкритого ключа не змінено на скасований або блокований з підстав, визначених цим Законом;
- за попередніми двома ознаками був чинним кваліфікований сертифікат відкритого ключа суб’єкта, який видав сертифікат.

3.8. Порядок виявлення будь-яких змін в електронному документі, в електронній копії з паперового документа після використання електронної печатки та порядок виявлення будь-яких

змін електронної печатки після її використання для засвідчення електронного документа, електронної копії з паперового документа

Накладання ЕП та електронної печатки унеможливлює внесення змін до електронного документа без порушення його структури таким чином, щоб електронний документ мав можливість зчитування загальним інструментарієм читання електронних файлів.

Сутність перевірки цілісності електронного документа, відсутність у цьому будь-яких змін після накладення ЕП та/або печатки полягає виключно у порівнянні часу підписання оригінального документа та документа, що перевіряється.

У разі виникнення розбіжностей між даними, вважається, що в електронний документ який перевіряється, було внесено несанкціоновані зміни.

У разі виявлення несанкціонованих змін в електронному документі після застосування ЕП та/або електронної печатки, проводиться внутрішнє службове розслідування та вживаються заходи щодо встановлення винних осіб та запобігання подібним ситуаціям у майбутньому.

Працівники Товариства, які безпосередньо у своїй діяльності створюють, супроводжують та підписують електронні документи, зобов'язані пересвідчитись, що в електронний документ після накладення ЕП та/або печатки не внесено зміни, бути уважними до підозрілих ознак або аномалій в електронних документах та негайно вживати заходів для їх виявлення та усунення у разі такого виявлення.

З метою можливості фіксування дій підписувача, повязаних зі створенням електронних документів, здійснення перевірки цілісності та моніторингу внесення змін до електронного документа, всі електронні документи Товариства реєструються в спеціальному електронному журналі.

4. ВИМОГИ ЩОДО НАДАННЯ, СКАСУВАННЯ ТА КОНТРОЛЮ ДОСТУПУ ДО ІНФОРМАЦІЙНИХ СИСТЕМ ТОВАРИСТВА, ЩО ВИКОРИСТОВУЮТЬСЯ ДЛЯ ПРИЙМАННЯ, РЕЄСТРАЦІЇ, ОБРОБЛЕННЯ ЗБЕРІГАННЯ ТА НАДСИЛАННЯ ЕЛЕКТРОННИХ ДОКУМЕНТІВ

З метою забезпечення безпеки та надійності інформаційних систем, що використовуються для оброблення електронних документів, запобіганню несанкціонованому доступу до даних та збереження конфіденційності та цілісності інформації в Товаристві встановлені вимоги щодо надання, скасування та контролю доступу до інформаційних систем Товариства, що використовуються для приймання, реєстрації, оброблення, зберігання, надсилання електронних документів, які містять:

- Вимоги до ідентифікації, автентифікації, авторизації клієнтів Товариства.

- Послідовність дій під час управління доступом, послідовність дій під час управління віддаленим доступом (реєстрація, надання повноважень, перегляд та скасування доступу).
- Перелік типових функцій та прав доступу до інформаційних систем Товариства.
- Вимоги щодо здійснення заходів контролю доступу.
- Періодичність контролю наданих прав доступу.
- Вимоги до протоколювання дій під час управління доступом.

4.1. Вимоги до ідентифікації, автентифікації, авторизації клієнтів Товариства

Товариство до встановлення ділових відносин, вчинення правочинів, проведення фінансової операції здійснює ідентифікацію та верифікацію клієнта з урахуванням вимог Закону України «Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення» та Положення про здійснення установами фінансового моніторингу.

Під час ідентифікації та верифікації резидентів Товариством встановлюються необхідні дані, визначені вимогами чинного законодавства України.

Клієнт надає Товариству необхідну інформацію для ідентифікації, верифікації, а також для подальшої автентифікації під час встановлення та підтримки ділових відносин.

Інформаційно-технічна система Товариства та працівники Товариства здійснюють всі необхідні заходи для належної перевірки Клієнта під час встановлення та підтримання ділових відносин.

Верифікація здійснюється відповідно до вимог Положення про здійснення установами фінансового моніторингу, затвердженого Постановою Правління
Національного банку України від 28.07.2020 № 107 та Правил здійснення фінансового моніторингу в ТОВ «АЛЕКСКРЕДИТ».

Для доступу до інформаційних систем Товариства, кожен користувач повинен пройти процес автентифікації.

Процес автентифікації відбувається шляхом введення ідентифікатора (логіна) користувача та пароля. Після успішної автентифікації Клієнту надається відповідний рівень доступу до функцій і даних Особистого кабінету, як частини інформаційно-технічної системи Товариства.

Для отримання кредиту Клієнт ідентифікується, виконує всі необхідні дії (підписує всі необхідні документи, в тому числі, електронні документи) на сайті та оформлює Заявку на сайті Товариства https://alexcredit.ua.

На підставі даних, зазначених у Заявці, на сайті Товариства здійснюється реєстрація Клієнта та створюється його Особистий кабінет.

Особистий кабінет створюється після підтвердження Товариством

можливості надання Клієнту Кредиту та зберігається в інформаційно-технічній системі Товариства після надання першого кредиту Клієнту та закривається за його вимогою, або у разі припинення ділових відносин з ним.

Доступ до Особистого кабінету (вхід в Особистий кабінет) здійснюється Клієнтом після автентифікації, яка проходить шляхом введення ідентифікатора (Логіна) і Пароля від Особистого кабінету.

Логін та Пароль Особистого кабінету самостійно встановлюється Клієнтом і складається з унікальної комбінації букв та/або цифр, яку останній зазначає в спеціальному полі «Логін» та «Пароль» при вході до Особистого кабінету.

Логін та Пароль Клієнт за власним бажанням може змінити.

Інформаційно-технічна система Товариства отримує інформацію щодо Логіну та Пароля Клієнта у токенізованому вигляді.

Пароль Клієнта залишається надійно захищеним та невидимим для всіх учасників інформаційно-технічної системи Товариства.

В Особистому кабінеті Клієнта відображається виключно та інформація, яка відноситься до даної особи та публічна інформація Товариства; доступ до особистих даних будь-яких інших осіб виключається.

Клієнтом в Особистому кабінеті можуть здійснюватися дії для отримання фінансової послуги (надання кредиту), комунікації з Товариством та управління особистими даними.

Клієнт має доступ до Особистого кабінету через мережу інтернет на сайті Товариства з будь-якого пристрою та будь-якої точки доступу.

4.2. Послідовність дій під час управління доступом, послідовність дій під час управління віддаленим доступом (реєстрація, надання повноважень, перегляд та скасування доступу Клієнта)

До інформаційно-технічної системи Товариства мають доступ Клієнти та працівники Товариства.

Кожен Клієнт має доступ виключно до інформації, що стосується тільки його особистості у обсягах, необхідних для ідентифікації та підтримання ділових відносин з Товариством. Клієнтам обмежений доступ до персональних даних та будь-якої іншої інформації інших осіб, окрім публічної інформації, розміщеної на сайті Товариства.

Клієнт отримує доступ до Особистого кабінету, як частини інформаційно-технічної системи Товариства, після верифікації, а саме: перед встановленням ділових відносин, а в подальшому - шляхом автентифікації на сайті Товариства.

Права доступу Клієнта до інформаційно-технічної системи Товариства обмежуються власним Особистим кабінетом. Клієнт не може здійснювати жодного інформаційного впливу на інформаційно-технічну систему Товариства.

Програмна структура інформаційно-технічної системи Товариства побудована таким чином, що унеможливлює та виключає доступ сторонніх осіб до її адміністративної частини та сприяє збереженню конфіденційності

та цілісності даних, а також захисту від несанкціонованого доступу та зловживань.

4.3 . Перелік типових функцій та прав доступу до інформаційних систем Товариства для працівників Товариства

Організаційна структура Товариства визначає спосіб організації та управління всіма аспектами діяльності підприємства. Ця структура включає в себе різні рівні управління, відповідальності та комунікації між різними Департаментами та їх працівниками.

Працівники Товариства мають доступ виключно до адміністративної частини інформаційно-технічної системи Товариства. Працівник окремого Департаменту має свої права доступу до інформаційно-технічної системи Товариства в межах та обсягах наданих повноважень та покладених на нього посадових і функціональних обов'язків.

Доступ до інформаційно-технічних систем Товариства працівники Товариства здійснюють через спеціальну CRM-систему. Кожен працівник має мінімальні права доступу, які йому необхідні для повноцінного виконання своїх посадових обов'язків.

У загальному випадку, повноваження та права доступу до інформаційно-технічної системи Товариства розподіляється за наступними напрямками:

- ***Клієнтська підтримка,*** яка включає здійснення належної перевірки Клієнта, встановлення та підтримання ділових відносин з Клієнтом, маркетингову взаємодію з Клієнтом протягом перших десяти днів прострочення зобов'язань за договором про надання кредиту, інші комунікації з Клієнтом.
- ***Колекторська діяльність*** – полягає у здійсненні взаємодії з Клієнтами з десятого дня прострочення зобов'язань за договором про надання кредиту та одночасним веденням всіх реєстраційних дій, передбачених чинним законодавством України.
- ***Юридичне забезпечення –*** забезпечується шляхом встановлення та підтриманням ділових відносин, наданням необхідної юридичної інформації, складанням юридичної звітності.
- ***Фінансово-економічний*** – полягає в узагальненні фінансової інформації при взаємодії з Клієнтами або контрагентами, формуванні звітності для організації бухгалтерського обліку.
- ***Маркетинговий*** – забезпечується здійсненням всіх видів взаємодії з Клієнтом щодо донесення інформації про можливість отримання кредиту, в тому числі, на пільгових умовах.
- ***Адміністративний*** – полягає у здійсненні контролю над усіма процесами; налаштуванні технологічних процесів; здійсненні контролю за діяльністю працівників Товариства та Клієнтів в інформаційно-технічній системі Товариства; налаштуванні та формуванні нефінансової звітності; наданні, перегляді та/ або скасуванні прав доступу та повноважень працівникам Товариства.

4.4. Вимоги щодо здійснення заходів контролю доступу

В Товаристві щодо кожного працівника здійснюється постійний контроль повноважень, який їм наданий для доступу до інформаційно-технічної системи Товариства. Програмним чином прописуються конкретні права на виконання певних функцій та зчитування певної інформації.

Усі дії працівників в інформаційно-технічній системі Товариства фіксуються спеціальними log-file, доступ до яких має виключно програміст та керівник Товариства.

У разі будь-якого порушення прав доступу до інформації, інформаційно-технічна система Товариства система автоматично зчитує даний факт і передає дану інформацію програмісту.

У разі виявлення фактів несанкціонованого доступу до інформаційно-технічної системи Товариства, проводиться внутрішнє службове розслідування, з метою з'ясування мети і причини такого доступу, встановлюються недоліки програмного забезпечення та винні особи.

За результатами проведеного службового розслідування керівником Товариства приймається рішення про застосування до винних працівників Товариства дисциплінарного стягнення, розробляються та вживаються відповідні заходи для запобігання подібним ситуаціям у майбутньому.

Клієнти мають доступ до інформаційно-технічної системи Товариства виключно в межах доступу до власного Особистого кабінету.

Забезпечення здійснення індивідуального доступу Клієнта до інформаційно-технічної системи Товариства відбувається шляхом його ідентифікації, верифікації та автентифікації.

Для виявлення фактів несанкціонованого доступу до інформаційно-технічної системи Товариства, включаючи спроби незаконного доступу, помилкові спроби входу та інші події, що стосуються безпеки, програмістом Товариства проводиться систематичний (один раз на тиждень) вибірковий моніторинг та аналіз.

З метою захисту персональних даних Клієнтів під час їх передачі та зберігання Товариство здійснює шифрування та токенізацію даних.

Для забезпечення здійснення належних заходів контролю доступу до інформаційно-технічної системи Товариства використовується спеціальне зовнішнє програмне забезпечення, яке забезпечує захист від хакерських атак.

Програмістом Товариства для підвищення рівня захисту інформаційно-технічної системи Товариства проводиться регулярне оновлення програмного забезпечення, систематично (1 раз на місяць) проводиться додаткове тестування працездатності серверів, на постійній основі здійснюється оцінка ризиків для мінімізації можливих загроз безпеці.

Інформаційно-технічна система Товариства здійснює комунікацію із зовнішніми серверами (Українське бюро кредитних історій, платіжні системи) виключно через API, які здійснюють обмін інформацією без доступу до системи Товариства.

Взаємодія сайту Товариства з інформаційно-технічною системою також здійснюється через механізми API та є захищеними додатковими зовнішніми сервісами.

Доступ до інформаційно-технічної системи реєструється спеціальним log-file, у якому вказується ім’я користувача та конкретна дія, яку він здійснив. Доступ до інформаційно-технічної системи обмежується доступом із фіксованої API адреси, що належить Товариству та унеможливлює доступ до системи сторонніх осіб.

Товариство для забезпечення належного функціонування інформаційно-технічної системи та захисту інформації, що обробляється в ній:

- створює резервну копію системи із дотриманням встановлених вимог щодо її захисту, цілісності та конфіденційності;
- забезпечує розміщення резервної копії на хмарних ресурсах.

Суворе дотримання перелічених вимог забезпечує надійний рівень захисту інформації та гарантує безпеку в інформаційно-технічній системі Товариства. Їх реалізація допомагає уникнути несанкціонованого доступу до даних та зберегти конфіденційність та цілісність інформації.

4.5. Періодичність контролю наданих прав доступу

Зміна, перегляд наданих прав доступу відбувається виключно на підставі виникнення змін у технологічних процесах в інформаційно-технічній системі Товариства.

Контроль за використанням наданих прав доступу в інформаційно-технічній системі Товариства забезпечується методом автоматизованого контролю.

Періодичність контролю наданих прав доступу у Товаристві не визначена, періодичний контроль за правами доступу не здійснюється.

Перегляд, зміна, додаткові налаштування прав доступу можливі за результатами проведеного службового розслідування у випадку фіксування фактів несанкціонованого доступу до інформаційно-технічної системи Товариства.

4.6.Вимоги до протоколювання дій під час управління доступом

Протоколювання дій під час управління доступом включає в себе реєстрацію всіх дій, пов'язаних з наданням, зміною та скасуванням доступу до ресурсів інформаційно-технічної системи, а також подій, пов'язаних з автентифікацією та авторизацією користувачів системи. Перелік основних вимог до протоколювання дій під час управління доступом:

Точність та повнота. Всі дії, пов'язані з управлінням доступом, повинні бути повністю та точно зареєстровані, включаючи надання, зміну та скасування прав доступу, а також всі взаємодії з системами автентифікації та авторизації.

Час та дата. Кожна подія управління доступом повинна бути маркована часом та датою її виникнення для забезпечення можливості

відстеження та аналізу подій у майбутньому.

Ідентифікація користувача. Всі дії повинні бути пов'язані з ідентифікацією конкретного користувача або облікового запису, щоб визначити, хто здійснював певні дії.

Опис дій. Кожна подія управління доступом повинна бути чітко описана, включаючи тип події (надання, зміна, скасування доступу), ідентифікатор ресурсу або облікового запису, до якого застосовується дія, та інші відомості, що характеризують дію.

Збереження та захист журналів подій. Протоколи подій повинні зберігатися в захищеному місці з обмеженим доступом для запобігання несанкціонованій зміні чи видаленню даних.

Моніторинг і аналіз. Зареєстровані події повинні бути доступні для моніторингу та аналізу з метою виявлення аномальних або небезпечних дій, а також для виконання аудиту безпеки.

Відповідність вимогам безпеки. Протоколювання дій повинно відповідати вимогам безпеки, встановленим внутрішніми політиками, законодавством та стандартами безпеки інформації.

Товариство дотримується принципу надання мінімального рівня повноважень під час надання доступу до інформаційних систем Товариства, що використовуються для приймання, реєстрації, оброблення, зберігання, надсилання електронних документів.

Вимоги даного Положення є обов’язковими для виконання всіма працівниками Товариства.

5. КОНТРОЛЬ ТА ВІДПОВІДАЛЬНІСТЬ

Директор Товариства відповідає за організацію використання ЕП та електронних печаток в Товаристві, а також за використання ЕП та електронних печаток уповноваженими працівники Товариства під час взаємодії від імені Товариства з клієнтами та/або контрагентами Товариства, якщо інше не встановлено законодавством України.

Відповідальність за забезпечення захисту інформації в інформаційно-технічній системі Товариства покладається на власника системи.

Особи, винні в порушенні законодавства про захист інформації в інформаційно-технічній системі, несуть відповідальність згідно із законом.

6. ЗАКЛЮЧНІ ПОЛОЖЕННЯ

Положення затверджується Рішенням Єдиного Учасника Товариства.

Дане Положення набирає чинності з дня його затвердження та діє до дати його скасування або затвердження нової редакції Положення. Нова редакція Положення припиняє дію попередньої редакції Положення з дати затвердження нової редакції Положення.

У разі невідповідності будь-якої частини Положення чинному законодавству України або іншим нормативним документам, на підставі яких розроблено Положення, зокрема, у зв’язку із внесенням до них змін /

введенням в дію нових законодавчих / нормативних документів, це Положення буде діяти лише в тій частині, яка не суперечитиме останнім.