ЗАТВЕРДЖЕНО
Рішенням Правління АТ «ОТП БАНК»
«25» червня 2018 року № 195

Публічна пропозиція АТ «ОТП БАНК» на укладення
Договору про нерозголошення інформації з обмеженим доступом

І. Загальні положення

1. АТ «ОТП БАНК» (далі - БАНК) відповідно до статей 638 та 641 Цивільного кодексу України оголошує Публічну пропозицію на укладення Договору про нерозголошення інформації з обмеженим доступом (далі - Договір) з метою встановлення з юридичними та фізичними особами (далі – Виконавець) договірних взаємовідносин Сторін щодо порядку використання Виконавцем ІзОД наданої БАНКОМ.

2. Ця Публічна пропозиція набирає чинності з дня її розміщення БАНКОМ на офіційному сайті БАНКУ за адресою: http://www.otpbank.com.ua, для ВИКОНАВЦЯ - із дня підписання ним Заяви про приєднання до умов Договору про нерозголошення інформації з обмеженим доступом (далі - Заява про приєднання), якщо інше не передбачено умовами Договору або зазначеною Заявою про приєднання та діє до прийняття Сторонами чи однією зі Сторін рішення про його розірвання або до дня офіційного оприлюднення БАНКОМ заяви про відкликання цієї Публічної пропозиції в цілому чи в частині на сторінці офіційного сайту БАНКУ.

3. Ця Публічна пропозиція не є публічним договором у розумінні статті 633 Цивільного кодексу України.

4. У цій Публічній пропозиції терміни вживаються в такому значенні

1) ІзОД – відомості, що містять банківську, комерційну таємниці, інсайдерську, конфіденційну інформацію, власником яких є Банк, або які є предметом професійного, ділового, виробничого, комерційного та/або інших інтересів Банку, а також персональні дані, стосовно яких згідно з положеннями Закону України «Про захист персональних даних» Банк виступає у ролі володільця.

2) Банківська таємниця – термін вживається згідно з визначенням, наведеним у статті 60 Закону України «Про банки і банківську діяльність».

3) Заява про приєднання - заява щодо акцептування цієї Публічної пропозиції (приєднання до Договору) за формою, наведеною в додатку 1 до Публічної пропозиції.

4) Інсайдерська інформація – термін вживається згідно з визначенням, наведеним у статті 44 Закону України «Про цінні папери та фондовий ринок».

5) Інформаційний актив (ресурс) – будь-яка сутність, що має для Банку цінність і впливає на властивості та рівень захисту інформації.

6) Комерційна таємниця – інформація, яка є секретною в тому розумінні, що вона в цілому чи в певній формі та сукупності її складових є невідомою та не є легкодоступною для осіб, які звичайно мають справу з видом інформації, до якого вона належить, у зв'язку з цим має комерційну цінність та була предметом адекватних існуючим обставинам заходів щодо збереження її секретності, вжитих особою, яка законно контролює цю інформацію. Комерційною таємницею можуть бути відомості технічного, організаційного, комерційного, виробничого та іншого характеру, за винятком тих, які відповідно до закону не можуть бути віднесені до комерційної таємниці. Перелік відомостей, що становлять комерційну таємницю Банку, наведено у розділі 3 цього Договору.

7) Конфіденційність – властивість інформації, яка полягає в тому, що інформація не може бути отримана неавторизованими користувачем і/або процесом без згоди Банку.

8) Персональні дані, база персональних даних, обробка персональних даних, володілець бази персональних даних – терміни вживаються згідно з визначеннями, наведеними в статті 2 Закону України «Про захист персональних даних».

9) Розголошення ІзОД – ознайомлення будь-якої особи з ІзОД, що відбулось з порушенням правового режиму доступу до цієї інформації.

10) Сторона – ВИКОНАВЕЦЬ або БАНК

11) Сторони- ВИКОНАВЕЦЬ та БАНК спільно.

12) Третя особа – будь-яка особа, за винятком Сторін.

5. **ІзОД** в себе також включає:

5.1.Банківська таємниця

Перелік відомостей, що становлять банківську таємницю, визначено статтею 60 Закону України «Про банки і банківську діяльність».

Зокрема до складу кодів, що використовуються Банком для захисту інформації і згідно з Законом України «Про банки і банківську діяльність» віднесені до банківської таємниці, входять:

- значення криптографічних ключів (за виключенням ключів несиметричних криптографічних алгоритмів, що передаються відкрито у складі сертифікатів), які використовуються для захисту платіжних документів та даних трансакцій платіжних систем і систем електронної комерції, а також для захисту платіжних продуктів (платіжні картки, електронні ваучери тощо);
- значення криптографічних ключів, що використовуються у засобах захисту інформації Банку або надані Банку Третіми особами у зв'язку зі здійсненням ним банківської діяльності;
- паролі, коди доступу до інформаційних активів Банку, засобів обмеження фізичного доступу, систем охоронної сигналізації Банку;
- коди, що використовуються для автентифікації та захисту даних платіжних карток національних та міжнародних платіжних систем і не є криптографічними ключами (PIN-коди, PIN-блоки, дані магнітних стрічок, особисті дані власників платіжних карток, що визначені міжнародним стандартом «Payment Card Industry Data Security Standard (PCI DSS)»).

5.2. Комерційна таємниця

До комерційної таємниці Банку віднесено такі відомості:

5.2.1. Відомості щодо організації банківських процесів, зокрема щодо:

- детальної структури Банку;
- масштабів діяльності Банку;
- типів та розміщення обладнання, що забезпечує виконання основних процесів Банку;
- детальні відомості стосовно топології комп'ютерної мережі Банку;
- узагальнені відомості про запаси матеріалів та комплектуючих, місця зберігання коштів та платіжних засобів, а також матеріалів, що використовуються для виготовлення або введення в обіг цих платіжних засобів.

5.2.2. Відомості щодо методів управління Банком та процесами банківської діяльності, зокрема щодо системи підпорядкування, заохочення працівників та контролю за їх діяльністю.

5.2.3. Відомості щодо тактичного планування та стратегії розвитку Банку.

5.2.4. Відомості щодо фінансового стану Банку, якщо вони не підлягають обов'язковому опублікуванню.

5.2.5. Відомості щодо маркетингових досліджень, що проведені Банком або отримані за його кошти.

5.2.6. Відомості щодо ринкової та цінової політики Банку.

5.2.7. Відомості щодо проведення торгів, зокрема відомості щодо підготовки до участі тендерах, а також результатів їх проведення.

5.2.8. Відомості щодо матеріалів робочих нарад та засідань.

5.2.9. Узагальнені відомості щодо партнерів та клієнтів, якщо ці відомості не віднесено до банківської таємниці і вони можуть бути використані для конкурентної боротьби проти Банку.

5.2.10. Відомості щодо переговорів та контрактів, зокрема про умови контрактів, господарських договорів, а також умови забезпечення конфіденційності, якщо вони розкривають зміст угоди або інші зобов'язання Банку перед партнерами та клієнтами.

5.2.11. Відомості щодо досліджень та розробок, зокрема:

- про мету, задачі, напрямки, програми перспективних досліджень щодо запровадження нових банківських продуктів і засобів автоматизації банківської діяльності, якщо ці відомості можуть бути використані для конкурентної боротьби проти Банку;
- ключові відомості про оригінальні ідеї технічних розробок, особливості організаційних, технологічних, конструктивних, технічних (у тому числі, програмно-апаратних), художньо-технічних рішень (наприклад, дизайну платіжних карток, оформлення реклами), які розроблено Банком самостійно або створено за його кошти.

5.2.12. Детальні відомості щодо технологій, зокрема про банківські технології та специфіку їх використання, у тому числі відомості щодо технології обробки інформації, виготовлення та введення в обіг платіжних засобів.

5.2.13. Інформація, що є об'єктом товарних відносин, зокрема інформація, яка надається партнерам та клієнтам Банку на комерційній основі, або яка придбана Банком за власні кошти (якщо умовами контрактів цю інформацію не визнано відкритою).

5.2.14. Відомості щодо організації та роботи системи безпеки Банку, якщо їх не віднесено до банківської таємниці, у тому числі відомості щодо інцидентів безпеки, що мали місце.

5.2.15. Відомості щодо авторського права, зокрема:

- відомості щодо політики управління авторським правом в Банку;
- відомості щодо планів, підготовки та результатів проведення переговорів з придбання авторських прав;

• особисті відомості про авторів, майнові авторські права яких передано Банку або використовуються Банком; • відомості про власників майнових прав, які передано Банку або використовуються Банком; • умови авторських договорів, які укладено Банком; • відомості, що розкривають зміст робіт зі створення продукції, майнові права на яку належать Банку (до їх офіційного оголошення). 5.2.16. Зміст розпорядчих та регулятивних документів, що містять рішення керівних органів Банку. 5.2.17. Перелік клієнтів Банку, якщо він містить інформацію стосовно 50 та більше осіб; 5.2.18. Інші відомості технічного, організаційного, комерційного, виробничого та іншого характеру, розголошення яких може призвести до суттєвого збитку Банку або погіршення його репутації.
5.3. Персональні дані
До ІзОД віднесено персональні дані співробітників Банку, клієнтів, інших фізичних осіб, володільцем яких є Банк.
5.4. Інсайдерська інформація
До ІзОД віднесено інсайдерську інформацію, яка знаходиться у розпорядженні Банку у зв'язку зі здійсненням своєї діяльності.
5.5. Конфіденційна інформація
Конфіденційна інформація – інформація про фізичну особу, а також інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень, що на законній підставі знаходиться у володінні, користуванні або розпорядженні Банку, доступ до якої обмежено Банком або іншими власниками цієї інформації (крім суб'єктів владних повноважень) і яка може поширюватися за рішенням Банку та/або бажанням (згодою) цих осіб у визначеному ними порядку та відповідно до передбачених ними умов. До конфіденційної інформації Банку зокрема відносяться: • зміст службової кореспонденції та інших внутрішніх документів Банку; • програмні коди та параметри налаштування систем обробки інформації Банку; • перелік клієнтів Банку, що стосується менш, як 50-ти осіб.

6. Інформація, яка не віднесена до ІзОД

Наступна інформація не вважається ІзОД і не є предметом Договору:

• інформація, доступ до якої не може бути обмежено згідно вимог законодавства України;

• інформація, офіційно оприлюднена Банком у відкритих засобах інформації, зокрема у засобах масової інформації;

інформація, щодо розкриття якої Виконавцю надано офіційний дозвіл Банку (у письмовій формі).

II. Порядок та умови укладення Договору

1. Укладенням Договору є акцептування цієї Публічної пропозиції (приєднання до Договору), що здійснюється ВИКОНАВЦЕМ, який підписав Заяву про приєднання відповідно до статті 634 Цивільного кодексу України, умови якого викладені в розділу III "Предмет та основні умови Договору" цієї Публічної пропозиції, за умови подання БАНКУ для перевірки документів, визначених БАНКОМ та законодавством України.

2. Приєднання ВИКОНАВЦЯ до цієї Публічної пропозиції відбувається в цілому, ВИКОНАВЕЦЬ не може запропонувати свої умови Договору.

3. БАНК у будь-який час протягом строку дії Договору має право запросити у ВИКОНАВЦЯ установчі та інші документи, визначені законодавством України. ВИКОНАВЕЦЬ зобов'язаний надавати БАНКУ запитані документи відповідно до пункту 3 розділу II цієї Публічної пропозиції.

4. Підписанням Заяви про приєднання ВИКОНАВЕЦЬ беззастережно підтверджує, що на час укладення Договору ВИКОНАВЕЦЬ ознайомився з повним текстом Договору, повністю зрозумів його зміст та погоджується з усіма його умовами, а також безумовно стверджує, що не позбавляється будь-яких прав, які має звичайно, а Договір не містить умов, які є для нього обтяжливими у будь-якому сенсі.

5. Акцептуючи цю Публічну пропозицію, ВИКОНАВЕЦЬ погоджується, що БАНК має право в будь-який час в односторонньому порядку вносити зміни до Договору, повідомляючи про це ВИКОНАВЦЯ офіційним опублікуванням тексту таких змін та нової редакції Договору на офіційному сайті БАНКУ. З часу набрання чинності зміни стають невід'ємною частиною Договору та обов'язковими до виконання для Сторін. Час опублікування на офіційному сайті БАНКУ є моментом ознайомлення ВИКОНАВЦЯ з текстом таких змін та погодження ним цих змін.

6. Зміни до Договору є прийнятними та погодженими ВИКОНАВЦЕМ (відповідно до частини третьої статті 205 Цивільного кодексу України), якщо протягом семи робочих днів із дня набрання ними чинності ВИКОНАВЕЦЬ не повідомить БАНК про розірвання Договору.

7. ВИКОНАВЕЦЬ погоджується з тим, що розміщення змін до Договору на офіційному сайті БАНКУ є належним виконанням останнім обов'язку щодо додержання форми та порядку повідомлення ВИКОНАВЦЯ про зміни до Договору.

8. ВИКОНАВЕЦЬ безумовно бере на себе ризики та обов'язок самостійно відстежувати є/немає повідомлень БАНКУ про зміни до Договору.

9. Сторони зобов'язуються без зволікань письмово інформувати одна одну про обставини, які мають значення для виконання умов Договору, у тому числі про зміну адрес та банківських реквізитів, перейменування Сторін, прийняття рішення про ліквідацію, реорганізацію або початок процедури банкрутства однієї зі Сторін, прийняття рішення щодо визнання ВИКОНАВЦЯ неплатоспроможним у строк не пізніше п'яти календарних днів із дня прийняття такого рішення.

10. Сторони безвідклично підтверджують, що уклали Договір, у тому числі на підставі принципу свободи договору, визначеного статтями 6 та 627 Цивільного кодексу України. Сторони також безвідклично підтверджують, що Договір не виключає / не обмежує відповідальність за порушення зобов'язань жодної зі Сторін.

11. ВИКОНАВЕЦЬ запевняє, що:

1) Договір не містить будь-яких обтяжливих умов для нього і є прийнятним у цілому з усіма умовами в редакції БАНКУ;

2) він ознайомлений зі змістом положень законодавства України, які передбачають відповідальність за правопорушення в сфері регулювання правовідносин, що є предметом Договору.

12. Сторони, укладаючи Договір, визначають, що всі спори, що виникають з приводу виконання Договору, вирішуються шляхом проведення взаємних переговорів. У разі недосягнення Сторонами згоди спір передається на вирішення до суду згідно із законодавством України.

13. Визнання недійсним будь-якої частини Договору не тягне за собою недійсності Договору в цілому. Визнання недійсним Договору не тягне за собою недійсності зобов'язань, які виникли між Сторонами на підставі обміну документами, що містять істотні умови Договору.

14. Договір є укладеним, а умови цієї Публічної пропозиції акцептованими ВИКОНАВЦЕМ з часу оформлення та підписання ним Заяви про приєднання за умови подання ВИКОНАВЦЕМ документів і відомостей, необхідних для підтвердження повноважень особи, яка підписала Заяву про приєднання, додатків до Договору за необхідністю та установчих документів ВИКОНАВЦЯ.

15. У разі наявності зауважень БАНКУ, які є перешкодою для укладення Договору, акцептування цієї Публічної пропозиції з боку ВИКОНАВЦЯ не є повним і таким, яке не створює юридичних наслідків. У цьому разі Договір є неукладеним та не створює зобов'язань для Сторін.

16. БАНК у будь-який час протягом строку дії Договору має право запросити у ВИКОНАВЦЯ установчі документи та підтвердження повноважень осіб, які підписують будь-які документи, пов'язані з Договором.

17. Ця Публічна пропозиція, оформлена ВИКОНАВЦЕМ Заява про приєднання, Договір, додатки до них - є єдиним документом.

18. Дата набрання чинності Договором визначається датою, яка міститься в розділі "Відмітки БАНКУ", у Заяві про приєднання, яка визначена та вписана в цей розділ відповідальним працівником БАНКУ за результатами розгляду документів, які подаються разом із Заявою про приєднання. Місцем укладення Договору є місцезнаходження БАНКУ.

III. Предмет та основні умови Договору

Стаття 1. Предмет Договору

1. Договір визначає порядок використання та збереження ВИКОНАВЦЕМ ІзОД переданого йому БАНКОМ, а також відповідальності ВИКОНАВЦЯ за порушення конфіденційності ІзОД.

Дія цього Договору також розповсюджується на ІзОД, що стала відома ВИКОНАВЦЮ у зв'язку зі здійсненням БАНКОМ своєї діяльності або наявністю між БАНКОМ та ВИКОНАВЦЕМ певних господарських або інших відносин, що регулюються законодавством України.

Стаття 2. Права та обов'язки Сторін

1. Права та обов'язки Сторін за Договором є комплексом зобов'язань БАНКУ та ВИКОНАВЦЯ, які передбачені Договором.

2. **ВИКОНАВЕЦЬ зобов'язується**:

2.1. Протягом всього строку дії та протягом 5 (п'яти) наступних послідовних років після закінчення дії цього Договору (або більш тривалого строку, якщо цей строк спеціально визначено законодавством України стосовно окремих категорій ІзОД):

2.1.1. Не розголошувати ІзОД Третім особам ІзОД, як вона визначена у цьому Договорі, без письмової згоди Банку.

2.1.2. Не надавати, не продавати Третім особам, не відчужувати у будь-який інший спосіб ІзОД.

2.1.3. Не використовувати ІзОД у будь-який спосіб, офіційно не дозволений Банком, зокрема не використовувати вищезазначену інформацію у власних інтересах або інтересах Третіх осіб.

2.1.3. Не використовувати ІзОД у будь-який спосіб, офіційно не дозволений Банком, зокрема не використовувати вищезазначену інформацію у власних інтересах або інтересах Третіх осіб.

2.1.4. Забезпечувати виконання вимог щодо режиму доступу, обробки та захисту ІзОД, визначених законодавством України та БАНКОМ, зокрема вимоги:

- Закону України «Про банки і банківську діяльність» – стосовно банківської таємниці;

• Закону України «Про захист персональних даних» – стосовно персональних даних, наданих Банком Виконавцю;

• Закону України «Про цінні папери та фондовий ринок» – стосовно інсайдерської інформації.

2.1.5. Не допускати несанкціонованого доступу до ІзОД неуповноважених осіб з числа співробітників ВИКОНАВЦЯ, а також Третіх осіб внаслідок незабезпечення належних заходів зберігання/режиму зберігання ІзОД, невжиття інших заходів обмеження доступу до ІзОД, які ВИКОНАВЕЦЬ повинен вжити з метою виконання умов цього Договору.

2.1.6. У строк, який є мінімально можливим, але не більше 24 годин з моменту настання події, інформувати БАНК про всі події, пов'язані з фактами розголошення або порушення конфіденційності ІзОД.

2.1.7. Дотримуватися Вимоги щодо забезпечення інформаційної безпеки Зовнішньою стороною, що залучається АТ «ОТП Банк» до виконання робіт (додаток №3 до Публічної пропозиції).

2.2. Забезпечити нерозголошення, вимог зазначених у п. 2.1 ст. 2 розділу ІІІ цього Договору, в т. ч. всіма співробітниками ВИКОНАВЦЯ, залученими ним до участі у переговорах з БАНКОМ, а також на співробітниками ВИКОНАВЦЯ, які у зв'язку з виконанням своїх службових обов'язків мають доступ до ІзОД.

Якщо до участі у переговорах з БАНКОМ ВИКОНАВЕЦЬ залучає осіб, що не перебувають з ВИКОНАВЦЕМ у трудових відносинах (на умовах договору підряду, договору послуг, авторських договорів. тощо), вимоги розділу п. 2.1. ст. 2 розділу ІІІ цього Договору у повній мірі розповсюджуються на таких залучених осіб.

Виконавець зобов'язаний довести вимоги цього Договору до осіб, зазначених у п. 2.2 ст. 2 розділу ІІІ цього Договору, шляхом підписання особистих зобов'язань за формою наведеною у Додатку №2 до Публічної пропозиції, з передачею одного екземпляра БАНКУ, за кожним особистим зобов'язанням.

2.3. У строк, який є мінімально можливим, але не більше 5 (п'яти) робочих днів після закінчення строку дії або припинення цього Договору, а також після отримання письмової вимоги БАНКУ, повернути БАНКУ носії ІзОД, не залишаючи у ВИКОНАВЦЯ жодних копій (у тому числі електронних), а також відтворень чи витягів з документів, файлів, даних тощо, які зазначені як ІзОД.

2.4. діяти згідно із законодавством України;

2.5. забезпечувати належне збереження наданих БАНКОМ програмних засобів і не передавати їх Третім особам;

2.6. своєчасно інформувати БАНК про зміни місцезнаходження, телефонів, прізвищ відповідальних осіб тощо. Обов'язково відповідати на запити БАНКУ щодо надання інформації, яка використовується для оперативної взаємодії з ВИКОНАВЦЕМ;**3. ВИКОНАВЕЦЬ має право:**

3.1. Використовувати ІзОД у зв'язку з установленням ділових відносин/співпраці чи інших відносин з БАНКОМ у спосіб, у межах та з метою, що офіційно дозволені БАНКОМ.

3.2. Надавати ІзОД уповноваженим державним органам на їх письмовий запит належної форми виключно у межах та випадках, передбачених законодавством України. Про кожний випадок отримання запиту на розкриття ІзОД Виконавець повинен не пізніше 24 годин з моменту отримання запиту направити відповідне письмове повідомлення БАНКУ.

4. БАНК має право:

4.1. Здійснювати аудит та моніторинг діяльності ВИКОНАВЦЯ, пов'язаної з доступом до ІзОД.

5. БАНК зобов'язаний:

5.1. діяти згідно із законодавством України;

Стаття 3. Відповідальність Сторін

1. За невиконання або неналежне виконання своїх зобов'язань однією із Сторін, передбачених Договором та законодавством України, винна Сторона несе відповідальність згідно з умовами Договору та законодавством України.

2. Сторона, яка порушила зобов'язання, взяті на себе за Договором, повинна усунути ці порушення в найкоротший строк.

3. Сплата штрафних санкцій (пені) не звільняє Сторони від виконання договірних зобов'язань.

4. ВИКОНАВЕЦЬ несе відповідальність:

4.1. ВИКОНАВЕЦЬ несе відповідальність за дії осіб, зазначені у п. 2.2 ст. 2 розділу ІІІ цього Договору.

4.2. За невиконання/неналежне виконання вимог п. 2. ст. 2 розділу ІІІ цього Договору ВИКОНАВЕЦЬ протягом 10 (десяти) днів з дати отримання вимоги Банку, сплачує Банку штраф у розмірі 100 000 (сто тисяч) гривень за кожний випадок порушення.

Крім того, БАНК має право додатково вимагати відшкодування ВИКОНАВЦЕМ, у повному обсязі, збитків завданих ВИКОНАВЦЕМ шляхом розголошенням ІзОД або порушенням вимог п. 2. ст. 2 розділу ІІІ цього Договору сума яких визначається за згодою Сторін або рішенням суду.

5. Кожна із Сторін несе відповідальність за збої в обміні інформацією, викликані навмисними, необережними або некомпетентними діями їх персоналу.

Стаття 4. Обставини непереборної сили (форс-мажор)

1. Сторони Договору звільняються від відповідальності за часткове або повне невиконання будь-якого з положень Договору, якщо це невиконання стало наслідком причин, що перебувають поза сферою контролю Сторони, яка його не виконала. Такі причини включають стихійне лихо, надзвичайні погодні умови, пожежі, війни, страйки, військові дії, громадські заворушення, але не обмежуються ними (далі - форс-мажор). Період

звільнення від відповідальності починається з часу оголошення однією Стороною форс-мажору і закінчується, якщо ця Сторона вжила заходів, яких вона і справді могла б ужити для виходу з форс-мажору. Форс-мажор автоматично продовжує строк виконання зобов'язань на весь період його дії та ліквідації наслідків. Про настання форс-мажорних обставин Сторони мають інформувати одна одну невідкладно. Якщо ці обставини триватимуть більше ніж шість місяців, то кожна зі Сторін матиме право відмовитися від подальшого виконання зобов'язань за цим Договором і в такому разі жодна зі Сторін не матиме права на відшкодування іншою Стороною можливих збитків.

2. Сторона, яка не може виконати своїх зобов'язань унаслідок надзвичайних обставин, передбачених у пункті 1 цієї статті, повинна письмово повідомити про це іншу Сторону протягом трьох робочих днів із часу виникнення цих обставин. Невиконання цієї вимоги не дає жодній із Сторін права посилатися надалі на вищезазначені обставини.

3. Належним доказом впливу дії обставин непереборної сили на можливість виконання Сторонами своїх зобов'язань за Договором є сертифікат Торгово-промислової палати України.

IV. Строк дії та припинення Договору

1. Строк дії цього Договору складає більший із вказаних нижче періодів:
   1.1. 5 (п’ять) років з дати набуття чинності Договору для ВИКОНАВЦЯ, або
   1.2. період з дати набуття чинності Договору для ВИКОНАВЦЯ і до завершення п’яти послідовних років з дати припинення договору за яким ВИКОНАВЕЦЬ надає БАНКУ послуги, поставляє товари, виконує роботи.

2. Договір може бути розірваний за згодою Сторін або з ініціативи БАНКУ в односторонньому порядку шляхом надсилання відповідного письмового повідомлення ВИКОНАВЦЮ.

3. Ініціювання розірвання цього Договору за ініціативою ВИКОНАВЦЯ можливе тільки за умови, якщо в ВИКОНАВЦЯ немає заборгованості перед БАНКОМ за цим Договором. Заборгованістю ВИКОНАВЦЯ є несплачені штрафних санкції, збитки відповідно до цього Договору.

4. Розірвання цього Договору, у тому числі за ініціативою БАНКУ, не звільняє ВИКОНАВЦЯ від обов'язку сплатити заборгованість, що виникла протягом дії цього Договору в повному обсязі.

5. Закінчення строку дії цього Договору не звільняє Сторони від виконання всіх передбачених цим Договором зобов’язань та від відповідальності за невиконання чи неналежне виконання зобов’язань в період дії Договору.

6. Договір припиняється у разі ліквідації Банку чи Виконавця.

V. Заключні положення

1. Усі зміни до Договору вносяться відповідно до умов Публічної пропозиції, повідомляючи про це ВИКОНАВЦЯ офіційним опублікуванням тексту таких змін (тобто нової редакції Договору чи його відповідної частини) на офіційному сайті БАНКУ.

2. Невиконання під час реалізації Договору однією із Сторін вимог іншої Сторони, які суперечать вимогам законодавства України, не може бути підставою для розірвання Договору.

3. ВИКОНАВЕЦЬ не має права на копіювання та/або розповсюдження, передавання третім особам програмно-технологічного забезпечення та інших об'єктів права інтелектуальної власності БАНКУ, отриманих у зв'язку з виконанням Договору.

4. Усі спори за Договором, що виникають з приводу виконання Договору, вирішуються шляхом проведення взаємних переговорів. У разі недосягнення Сторонами згоди спір передається на вирішення до суду згідно із законодавством України.

5. Усі додатки та доповнення є невід’ємною частиною Договору.

VI. Місцезнаходження та реквізити Сторін

Місцезнаходження: 01033, м. Київ, вул. Жилянська, 43
Поштова адреса: 01601, м. Київ, вул. Жилянська, 43
Код за ЄДРПОУ: 21685166
Індивідуальний податковий номер_____

VII. Реквізити БАНКУ

Рахунок БАНКУ: п/р _____.
Код банку 300528

Додаток 1
до Публічної пропозиції АТ «ОТП БАНК» на укладення Договору про нерозголошення інформації з обмеженим доступом

Заява про приєднання до умов Договору про нерозголошення інформації з обмеженим доступом
N _____ від "___" _____ 20__ року

Повне найменування ВИКОНАВЦЯ:	
Код за ЄДРПОУ:	
п/р:	
Код банку:	
ІПН:	
Місцезнаходження:	
В особі:	
Контактні телефони:	

1. Керуючись статтею 634 Цивільного кодексу України, шляхом подання Заяви про приєднання до умов Договору про нерозголошення інформації з обмеженим доступом (надалі – Заява про приєднання) ВИКОНАВЕЦЬ приєднується до установлених БАНКОМ умов Договору про нерозголошення інформації з обмеженим доступом (далі - Договір), розміщених на офіційному сайті БАНКУ за адресою: http://otpbank.com.ua.

2. Датою приєднання до Договору є дата, яка міститься в розділі "Відмітки БАНКУ", визначена та вписана в цей розділ відповідальним працівником БАНКУ після опрацювання заяви та за умови, якщо немає зауважень до поданих ВИКОНАВЦЕМ документів.

3. ВИКОНАВЕЦЬ засвідчує, що він ознайомився з умовами Договору розміщеному на офіційному сайті БАНКУ, погоджується з ними та зобов'язується його виконувати.

4. Підписанням Заяви про приєднання ВИКОНАВЕЦЬ беззастережно підтверджує, що на момент укладення цього ВИКОНАВЕЦЬ ознайомився з його повним текстом, повністю зрозумів його зміст та погоджується з усіма умовами цього Договору, а також безумовно стверджує, що не позбавляється будь-яких прав, які має звичайно, а цей Договір не містить умов, які є для нього обтяжливими в будь-якому сенсі.

5. Підписуючи заяву, ВИКОНАВЕЦЬ погоджується, що БАНК має право в будь-який час в односторонньому порядку вносити зміни до Договору, повідомляючи про це ВИКОНАВЦЯ офіційним опублікуванням тексту таких змін (тобто нової редакції Договору чи його відповідної частини) на офіційному сайті БАНКУ. З моменту набрання чинності зміни стають невід'ємною частиною Договору та обов'язковими до виконання для сторін. Момент здійснення опублікування на офіційному сайті БАНКУ є моментом ознайомлення ВИКОНАВЦЯ з текстом таких змін та узгодження ним цих змін.

6. Підписанням цієї Заяви про приєднання ВИКОНАВЕЦЬ беззастережно підтверджує, що розміщення змін до цього Договору на офіційному сайті БАНКУ є належним виконанням останнім обов'язку щодо додержання форми та порядку повідомлення ВИКОНАВЦЯ про зміни Договору. ВИКОНАВЕЦЬ безумовно бере на себе ризики та обов'язок самостійно відстежувати наявність повідомлень БАНКУ про зміну умов цього Договору.

7. Підписанням Заяви про приєднання ВИКОНАВЕЦЬ підтверджує те, що: Я, Власник персональних даних (особа, уповноважена ВИКОНАВЦЕМ на підписання даної Заяви про приєднання), повідомлений про мету обробки БАНКОМ моїх персональних даних (будь-яка інформація про фізичну особу або інформація, що стосується фізичної особи, в тому числі, однак не виключно інформація щодо прізвища, імені, по батькові, даних, які зазначені в паспорті (або даних, які зазначені в іншому документі, що посвідчує особу), реєстраційного номеру облікової картки платника податків, громадянства, місця проживання або перебування, місця роботи, посади, номерів контактних телефонів/факсів, адреси електронної пошти, тощо, надалі – «Персональні дані»), а саме: укладення, зміни, припинення договорів, виконання договорів, а також для здійснення дій, пов’язаних із укладенням, зміною, припиненням та/або виконанням договорів, у тому числі шляхом здійснення прямих контактів із Власником персональних даних за допомогою засобів зв’язку; захист БАНКОМ своїх прав та інтересів.

Підписанням даної Заяви про приєднання Власник персональних даних надає БАНКУ свою однозначну згоду на передачу (поширення), у т.ч. транскордонну, БАНКОМ Персональних даних третім особам (особи, з якими БАНК перебуває в договірних відносинах та/або члени Групи ОТП), зміну, знищення Персональних даних або обмеження доступу до них відповідно до вимог Закону України «Про захист персональних даних» від 01.06.2010 року (надалі – «Закон») та без необхідності надання Власнику персональних даних письмового повідомлення про здійснення зазначених дій.

Підписанням даної Заяви про приєднання Власник персональних даних підтверджує, що в момент збору Персональних даних БАНК повідомив його про володільця Персональних даних, склад та зміст зібраних Персональних даних, права, передбачені Законом, про мету збору Персональних даних та осіб, яким передаються його Персональні дані.

ВИКОНАВЕЦЬ підтверджує (гарантує), що Персональні дані фізичних осіб, які передаються БАНКУ, здійснюється за згодою таких фізичних осіб які повідомлені про відомості, зазначені в ч.2 ст.12 Закону.

Застереження: Термін "оброблення персональних даних" визначається законодавством України, зокрема Законом.

Посада уповноваженої особи	Підпис М. П.	Прізвище, ім'я, по батькові уповноваженої особи

ВІДМІТКИ БАНКУ		

Відповідальні особи ВИКОНАВЦЯ:

_____
_____
_____
_____
_____
_____
_____

Додаток 2
до Публічної пропозиції АТ «ОТП БАНК» на укладення Договору про нерозголошення інформації з обмеженим доступом

Особисті зобов'язання
щодо нерозголошення інформації з обмеженим доступом та дотримання вимог безпеки АТ «ОТП Банк»

Я, _____ ,
зазначити П.І.Б. без скорочень, серію та номер паспорта громадянина України, іншого паспортного документа іноземця чи особи без громадянства, ким і коли був виданий

співробітник _____ ,
зазначити назву організації

що діє згідно з договором _____ (далі – Договір виконання робіт) ,
зазначити реквізити договору

укладеним між АТ «ОТП Банк» (далі – Банк) та _____ (далі – Виконавець)
зазначити назву організації

наступним підтверджую, що мені були роз'яснені та є зрозумілими вимоги Договору щодо нерозголошення інформації з обмеженим доступом та дотримання вимог безпеки АТ «ОТП Банк»
_____
зазначити реквізити договору

(далі – Договір щодо нерозголошення), укладеному між Банком та Виконавцем
та Вимоги щодо забезпечення інформаційної безпеки Зовнішньою стороною, що залучається АТ «ОТП Банк» до виконання робіт (додаток №3 до Публічної пропозиції АТ «ОТП БАНК» на укладення Договору про нерозголошення інформації з обмеженим доступом).

Я зобов'язуюсь:

1. Протягом всього строку дії та протягом 5 (п'яти) наступних послідовних років після закінчення дії цього Договору (або більш тривалого строку, якщо цей строк спеціально визначено законодавством України стосовно окремих категорій інформації з обмеженим доступом):
- не розголошувати інформацію з обмеженим доступом (у тому числі відомості, що містять банківську таємницю, комерційну таємницю, конфіденційну та інсайдерську інформацію, персональні дані клієнтів та співробітників Банку), власником якої є Банк або які є предметом професійного, ділового, виробничого, комерційного та інших інтересів Банку (далі – **ІзОД**), яка була доведена мені у встановленому Банком порядку або стала відома у зв'язку з виконанням моїх обов'язків;
- не використовувати ІзОД у власних інтересах або на інтересах третіх осіб;
- своєчасно та у повному обсязі виконувати усі вимоги щодо забезпечення інформаційної безпеки, визначені Банком;
- по закінченню виконання робіт, обумовлених Договором виконання робіт, повернути Банку всі носії ІзОД, що є власністю або знаходяться у розпорядженні Банку і надані мені у зв'язку з виконанням моїх обов'язків або фактично знаходяться у моєму розпорядженні;
- знищити всі копії даних та документів, які містять ІзОД, якщо такі копії тимчасово використовувались мною під час виконання робіт, у спосіб, що гарантує неможливість відновлення цієї інформації.

2. Під час перебування на території Банку виконувати доведені мені правила внутрішнього розпорядку та режиму безпеки Банку.

2.1. Не здійснювати несанкціонованого втручання та спроби втручання в роботу автоматизованих систем обробки інформації Банку (у тому числі шляхом умисного розповсюдження шкідливого програмного коду), а також спроби несанкціонованого перехоплення, пересилання або копіювання інформації, що оброблюється цими системами.

2.2. Дотримуватись правил інформаційної безпеки на комп'ютері, з якого здійснюється підключення до інформаційних ресурсів Банку.

Мене попереджено про відповідальність згідно з законодавством України відповідальність за неправомірне розголошення або використання інформації з обмеженим доступом, а також за порушення роботи та несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку Банку. .

Я погоджуюсь із тим, що вся інформація, створена мною в межах Банку за умовами Договору виконання робіт, є власністю Банку, та даю згоду на використання цієї інформації Банком відповідно до внутрішніх процедур.

Підписанням цього Зобов'язання надаю свою добровільну та однозначну згоду на обробку Банком моїх персональних даних,(будь-якої інформації, що стосується мене, а саме: прізвища, власного імені, по батькові, дати та місця народження, серії та номеру паспорта (або іншого документу, що посвідчує особу) дату видачі та органу, що його видав, ідентифікаційного номеру (індивідуального податкового номеру), адреси (місце проживання або перебування), освіти, професії тощо (надалі - "Персональні дані")), наданих Банку у зв'язку з укладенням Договору виконання робіт та/або пов'язані з моєю роботою в Банку, з метою забезпечення реалізації Банком відносин, що

виникають на основі Договору виконання робіт, здійснення ним прав, захисту своїх інтересів та виконання обов'язків за цим Договором, а також з метою забезпечення моєї персональної безпеки і безпеки Банку.
Також, надаю Банку свою однозначну згоду на передачу (поширення), у т.ч. транскордонну, Банком моїх Персональних даних Третім особам (особи, з якими Банк перебуває в договірних відносинах, а також члени Групи ОТП) або обмеження доступу до них відповідно до вимог Закону України «Про захист персональних даних» від 01.06.2010 року (надалі – «Закон») та без необхідності надання мені письмового повідомлення про здійснення зазначених дій.
Підтверджую, що мене повідомлено належним чином про володільця Персональних даних, склад та зміст зібраних Персональних даних, мої права, передбачені Законом, мету збору моїх Персональних даних та осіб, яким передаються мої Персональні дані, засвідчую, що склад та зміст Персональних даних є відповідним визначеній вище меті обробки персональних даних. При цьому терміни «персональні дані» та «обробка персональних даних» я розумію у редакції, наведеній у статті 2 Закону України «Про захист персональних даних».

Ця Зобов’язання складено у трьох примірниках, що мають однакову юридичну силу. Один з примірників надається Банку, другій – особі, що склала це Зобов’язання, третій – Виконавцю.

_____ (дата) _____ (підпис)

Додаток 3 до Публічної пропозиції АТ «ОТП БАНК» на укладення Договору про нерозголошення інформації з обмеженим доступом

Вимоги щодо забезпечення інформаційної безпеки Зовнішньою стороною, що залучається АТ «ОТП Банк» до виконання робіт

1. Терміни та скорочення, що використовуються в даному документі

Банк – АТ «ОТП БАНК»;

Договір – договір цивільно-правового (господарського) характеру (договір підряду, договір про надання послуг тощо), на підставі якого Зовнішня сторона залучається Банком до виконання робіт, надання послуг, поставку товару.

ІБ – інформаційна безпека;

ІзОД – інформація з обмеженим доступом.

Автентифікація користувача – процедура перевірки відповідності пред'явленого ідентифікатора користувача на предмет належності цьому користувачеві; встановлення або підтвердження справжності користувача.

Аутсорсинг – передача Зовнішній стороні певних бізнес-функцій або складових бізнес-процесу Банку з метою підвищення продуктивності праці або зниження собівартості послуг.

Аутстаффінг – виведення персоналу за штат Банку, що передбачає використання Банком послуг робітників, які юридично є представниками Зовнішньої сторони.

Банківська таємниця – інформація щодо діяльності та фінансового стану клієнта, яка стала відомою банку у процесі обслуговування клієнта та взаємовідносин з ним чи третім особам при наданні послуг банку (Закон України «Про банки і банківську діяльність»).

Виконавець - надалі також Зовнішня сторона.

Вразливість – нездатність протистояти реалізації певної загрози або сукупності загроз.

Доступність – властивість ресурсу системи обробки інформації, яка полягає в тому, що користувач і/або процес, який володіє відповідними повноваженнями, може використовувати ресурс відповідно до правил, встановлених політикою безпеки, не очікуючи довше заданого (малого) проміжку часу, тобто коли він знаходиться у вигляді, необхідному користувачеві, в місці, необхідному користувачеві, і в той час, коли він йому необхідний.

Договір про надання послуг – договір, що укладається між Банком та Зовнішньою стороною про надання послуг, виконання робіт, поставки товару у галузі інформаційних технологій, пов'язаних з банківською діяльністю.

Загроза ІБ – будь-яка обставина або подія ІБ, що можуть бути причиною порушення політики безпеки інформації або нанесення збитків Банку.

Захист інформації – сукупність правових, адміністративних, організаційних, технічних та інших заходів, що забезпечують збереження, цілісність інформації та належний порядок доступу до неї (Закон України «Про інформацію»).

Зовнішня сторона (у контексті цих Вимог) – фізичні або юридичні особи, організації, які не асоціюються з Банком та залучаються Банком до виконання робіт, надання послуг, постачання товарів на підставі договорів цивільно-правового (господарського) характеру.

Ідентифікатор – унікальний атрибут (ім'я) об'єкта (користувача, процесу), що дозволяє однозначно виділити даний об'єкт серед подібних.

Інсайдерська інформація – неоприлюднена інформація про емітента, його цінні папери та похідні (деривативи), що перебувають в обігу на фондовій біржі, або правочини щодо них, у разі якщо оприлюднення такої інформації може істотно вплинути на вартість цінних паперів та похідних (деривативів), та яка підлягає оприлюдненню відповідно до вимог, встановлених цим Законом. Інформація щодо оцінки вартості цінних паперів та/або фінансово-господарського стану емітента, якщо вона отримана виключно на основі оприлюдненої інформації або інформації з інших публічних джерел, не заборонених законодавством, не є інсайдерською інформацією. Інформація не вважається інсайдерською з моменту її оприлюднення відповідно до закону (Закон України «Про цінні папери та фондовий ринок»).

Інформаційна безпека Банку – стан інформації, в якому забезпечується збереження конфіденційності, цілісності та доступності інформації, а також цілісності, спостереженості та керованості процесів її обробки згідно з вимогами, визначеними політикою ІБ Банку.

Інформаційний ресурс – будь-яка сутність, що має для Банку цінність і впливає на властивості та рівень захисту інформації. До інформаційних ресурсів зокрема належать: власне інформація, обладнання, програмні ресурси, інженерна інфраструктура, інформаційні послуги та сервіси життєзабезпечення, персонал, причетний до обробки інформації тощо.

Інформаційна система (система інформаційних технологій) - організаційно-технічна система, в якій реалізується технологія обробки інформації з використанням технічних і програмних засобів, зокрема, САБ, системи зв'язку тощо; **Інформація** – будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді (Закон України «Про інформацію»).

Інформація з обмеженим доступом – відомості, що містять банківську, комерційну таємниці, конфіденційну, інсайдерську інформацію, власником яких є Банк, або які є предметом професійного, ділового, виробничого, комерційного та інших інтересів Банку, інформація, яка стосується здійснення Банком фінансового моніторингу,

а також персональні дані, стосовно яких згідно з положеннями Закону України «Про захист персональних даних» Банк виступає у ролі володільця, розпорядника персональних даних або у ролі третьої особи. Перелік ІзОД Банку та порядок її визначення наведено в регуляторному документі Банку «Положення про класифікацію інформації та заходи щодо забезпечення захисту інформації з обмеженим доступом».

Інцидент інформаційної безпеки – поява однієї або кількох небажаних або непередбачених подій ІБ, з якими пов'язана значна ймовірність компрометації процесів банківської діяльності та створення загроз ІБ.

Комерційна таємниця – інформація, яка є секретною в тому розумінні, що вона в цілому чи в певній формі та сукупності її складових є невідомою та не є легкодоступною для осіб, які звичайно мають справу з видом інформації, до якого вона належить, у зв'язку з цим має комерційну цінність та була предметом адекватних існуючим обставинам заходів щодо збереження її секретності, вжитих особою, яка законно контролює цю інформацію. Комерційною таємницею можуть бути відомості технічного, організаційного, комерційного, виробничого та іншого характеру, за винятком тих, які відповідно до закону не можуть бути віднесені до комерційної таємниці (Цивільний кодекс України).

Конфіденційна інформація – інформація про фізичну особу, а також інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень. Конфіденційна інформація може поширюватися за бажанням (згодою) відповідної особи у визначеному нею порядку відповідно до передбачених нею умов, а також в інших випадках, визначених законом (Закон України «Про інформацію»).

Конфіденційність – властивість інформації, яка полягає в тому, що інформація не може бути отримана неавторизованим користувачем і/або процесом.

Правила інформаційної безпеки – приписи, інструкції, регламенти, вимоги, рекомендації щодо забезпечення безпеки інформації, які містяться у стандартах України, міжнародних стандартах сімейства ISO/IEC 27000, стандартах платіжних систем, національних документах інших країн, міжнародних науково-дослідних організацій та професійних об'єднань.

Персональні дані – відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована (Закон України «Про захист персональних даних»). До конфіденційної інформації про фізичну особу належать, зокрема, дані про її національність, освіту, сімейний стан, релігійні переконання, стан здоров'я, а також адреса, дата і місце народження (Закон України «Про інформацію»).

Система автоматизації банку – система інформаційних технологій, що вирішує задачі автоматизації банківської діяльності (наприклад, система «Операційний день банку», система «Клієнт-банк» тощо).

Спостережність – властивість системи обробки інформації, що дозволяє фіксувати діяльність користувачів і процесів, використання пасивних об'єктів, а також однозначно установлювати ідентифікатори причетних до певних подій користувачів і процесів з метою запобігання порушення політики безпеки і/або забезпечення відповідальності за певні дії.

Стеганографія – тайнопис, при якому повідомлення закодоване таким чином, що не виглядає як повідомлення.

Третя сторона – фізична або юридична особа, організація, орган державної влади тощо, які не асоціюються з Банком або особами, що перебувають у ділових відносинах з Банком у зв'язку зі здійсненням банківської діяльності.

Цілісність інформації – властивість інформації, яка полягає в тому, що інформація не може бути модифікована неавторизованим користувачем і/або процесом.

Цілісність системи – властивість системи, яка полягає в тому, що жоден її компонент не може бути усунений, модифікований або доданий з порушенням політики безпеки.

2. Вимоги інформаційної безпеки

2.1. Доступ Зовнішній стороні до інформаційних ресурсів та приміщень Банку, де ці ресурси розміщено, надається виключно з дозволу і в інтересах Банку у зв'язку зі здійсненням ним банківської діяльності.

2.2. Загальною підставою для надання доступу є Договір про надання послуг, укладений між Банком та Зовнішньою стороною.

2.3. У випадку, якщо в процесі підготовки або виконання умов Договору про надання послуг, Зовнішня сторона отримує можливість доступу до ІзОД та інформаційних ресурсів Банку, Зовнішня сторона зобов'язана дотримуватись в ході співробітництва з Банком вимог щодо конфіденційності та інформаційної безпеки.

2.3.1. Зобов'язання Зовнішньої сторони щодо дотримання в ході співробітництва з Банком вимог щодо конфіденційності та інформаційної безпеки фіксуються шляхом приєднання до Договору про конфіденційність, який є договором публічної оферти і публікується на сайті Банку.

2.3.2. Вимоги інформаційної безпеки щодо Зовнішньої сторони визначаються регулятивними документами банку (політиками, положеннями, регламентами, інструкціями, порядками тощо) щодо забезпечення інформаційної безпеки і включають (але не обмежуючись):

- визначення ІзОД, що є предметом цього договору про конфіденційність;
- цінність для Банку та конфіденційність залученої інформації;
- відповідальність та дії Зовнішньої сторони щодо запобігання несанкціонованому розголошенню ІзОД;
- право власності на інформацію у тому числі, право інтелектуальної власності;
- дозволені способи використання Зовнішньою стороною ІзОД Банку;
- процедуру сповіщення та звітування щодо фактів розголошення або порушення конфіденційності ІзОД Банку.
- перелік інформаційних ресурсів Банку, до яких надається доступ Зовнішній стороні;
- спосіб та термін надання доступу Зовнішній стороні до інформаційних ресурсів Банку;

- спосіб ідентифікації співробітників Зовнішньої сторони, а також порядок санкціонування, верифікації, перегляду та скасування прав доступу до інформаційних ресурсів Банку;
- інциденти ІБ, що можуть мати місце, та порядок реагування на інциденти;
- заходи безпеки, які мають бути застосовані Зовнішньою стороною для захисту інформаційних ресурсів Банку.
- заходи безпеки, які мають бути застосовані Зовнішньою стороною для захисту власних інформаційних ресурсів з метою унеможливлення шкоди інформаційним ресурсам Банку.

2.4. У випадках, якщо послуги Зовнішньої сторони:
- надаються на умовах аутстаффінгу;
- передбачають створення окремих робочих місць або присутність представників Зовнішньої сторони на території Банку;
- надання представникам Зовнішньої сторони віддаленого доступу до ресурсів, розміщених в інформаційній мережі Банку,

до моменту фактичного надання доступу Зовнішній стороні до інформаційних ресурсів Банку повинні бути виконані такі умови:
- підписання вищезазначеними представниками Зовнішньої сторони особистих зобов'язань щодо нерозголошення ІзОД та дотримання вимог безпеки АТ «ОТП Банк» (Додаток 2 до Публічної пропозиції);
- надання Зовнішньою стороною клопотання (у формі офіційного листа) щодо забезпечення її представникам віддаленого доступу до інформаційних ресурсів Банку або організації робочих місць та надання доступу до службових приміщень Банку та підтвердження дотримання правил інформаційної безпеки на комп'ютерах, з яких її представники підключатимуться до інформаційних ресурсів банку.

2.5. Представники Зовнішньої сторони **ЗОБОВ'ЯЗАНІ**:

2.5.1. Знати та виконувати вимоги ІБ, що їх стосуються, визначені Договором, у тому числі на комп'ютерах, з яких відбувається підключення до інформаційних ресурсів банку.

2.5.2. Знати та виконувати вимоги щодо забезпечення режиму конфіденційності ІзОД Банку, визначені договором про конфіденційність. Не розголошувати ІзОД (у тому числі відомості, що містять банківську таємницю, комерційну таємницю, конфіденційну та інсайдерську інформацію, персональні дані клієнтів та співробітників Банку), власником якої є Банк або які є предметом професійного, ділового, виробничого, комерційного та інших інтересів Банку, яка була доведена представнику у встановленому Банком порядку або стала відома у зв'язку з виконанням представником його обов'язків.

2.5.3. Не допускати несанкціонованого доступу до ІзОД неуповноважених осіб з числа співробітників Виконавця, а також Третіх осіб внаслідок незабезпечення належних заходів зберігання/режиму зберігання ІзОД, невжиття інших заходів обмеження доступу до ІзОД, які Виконавець повинен вжити з метою виконання умов цього Договору.

2.5.4. Своєчасно та у повному обсязі виконувати заходи, визначені Банком, щодо запобігання несанкціонованого доступу до ІзОД, безпечного використання та збереження інформаційних ресурсів Банку, які були надані Зовнішній стороні у зв'язку з виконанням Договору.

2.5.5. Під час перебування на території Банку виконувати доведені до представника Зовнішньої сторони правила внутрішнього розпорядку та режиму безпеки Банку.

2.5.6. Знати перелік інформаційних ресурсів Банку, до яких представнику Зовнішньої сторони надається доступ, а також дозволені методи та регламент доступу, включаючи терміни початку надання та припинення доступу.

2.5.7. Знати та виконувати вимоги Банку щодо дозволу або заборони здійснення Зовнішньою стороною процесів управління змінами інформаційних ресурсів Банку (оновлення програмного та апаратного забезпечення, зміна конфігурації засобів обробки інформації тощо) та керування вразливостями (у тому числі, вимоги щодо здійснення процесу сканування ресурсів інформаційної мережі, підтримка яких здійснюється на умовах аутсорсингу), а також порядок виконання таких дій, що стосуються представника Зовнішньої сторони (у випадку наявності відповідного дозволу).

2.5.8. Виконувати вимоги Банку, які стосуються представників Зовнішньої сторони, стосовно ідентифікації та автентифікації під час здійснення логічного доступу до інформаційної мережі та інформаційних систем Банку (зокрема вимоги щодо застосування унікальних ідентифікаторів та паролів доступу).

2.5.9. По закінченню виконання робіт, обумовлених Договором, повернути Банку всі носії ІзОД, що є власністю або знаходяться у розпорядженні Банку і були надані представнику у зв'язку з виконанням представником його обов'язків або фактично знаходяться у розпорядженні представника. Знищити всі копії даних та документів, які містять ІзОД, у спосіб, що гарантує неможливість відновлення цієї інформації, якщо такі копії тимчасово використовувались під час виконання робіт.

2.5.10. Знати спосіб, у який мають здійснюватись комунікації з Банком у випадку виникнення інцидентів ІБ та надзвичайних ситуацій. Негайно інформувати Банк стосовно фактів виникнення інцидентів ІБ або надзвичайних ситуацій, що мають відношення до виконання робіт, обумовлених Договором.

2.6. Представникам Зовнішньої сторони **ЗАБОРОНЯЄТЬСЯ**:

2.6.1. Розголошувати ІзОД (у тому числі відомості, що містять банківську таємницю, комерційну таємницю, конфіденційну та інсайдерську інформацію, персональні дані клієнтів та представників Банку), власником якої є Банк або які є предметом професійного, ділового, виробничого, комерційного та інших інтересів Банку, яка була доведена представнику у встановленому Банком порядку або стала відома у зв'язку з виконанням представником його обов'язків.

2.6.2. Використовувати ІзОД Банку у власних інтересах або в інтересах третіх осіб.
2.6.3. Здійснювати доступ до інформаційних ресурсів, а також виробничих приміщень Банку у спосіб, який не дозволено Банком (при цьому слід керуватись принципом, «дії, які не дозволені Банком, вважаються забороненими»).
2.6.4. Використовувати з метою здійснення доступу до інформаційних ресурсів та виробничих приміщень Банку будь-які персональні атрибути доступу (ідентифікатори, паролі, коди, перепустки тощо), які належать іншій особі, а також надавати власні атрибути доступу будь-яким іншим особам.
2.6.5. Здійснювати несанкціоноване Банком втручання в роботу комп'ютерів, інформаційних систем, комп'ютерних мереж чи мереж електрозв'язку Банку.
2.6.6. Здійснювати несанкціоновані Банком зміну, знищення або блокування інформації, яка оброблюється в комп'ютерах, інформаційних системах чи комп'ютерних мережах Банку або зберігається на носіях такої інформації.
2.6.7. Здійснювати несанкціоновані Банком дії, спрямовані на отримання ІзОД Банку, у тому числі шляхом перехоплення або копіювання інформації, яка оброблюється в комп'ютерах, інформаційних системах, комп'ютерних мережах Банку або зберігається на носіях такої інформації (зокрема засобами технічної розвідки, шляхом фотографування документів та пристроїв відображення інформації, шляхом застосування пристроїв аудіозапису тощо).
Здійснювати несанкціоновані Банком дії, спрямовані на отримання інформації щодо топології комп'ютерних мереж, а також конфігурації, параметрів, ідентифікаторів доступу мережевих ресурсів та пристроїв Банку, у тому числі із застосуванням мережевих сканерів.
2.6.8. Порушувати правила експлуатації комп'ютерів, інформаційних систем, комп'ютерних мереж чи мереж електрозв'язку Банку або порядку чи правил захисту інформації, яка в них оброблюється.
2.6.9. Навмисно або ненавмисно розповсюджувати в середовищі Банку шкідливі програмні засоби, застосовувати (у тому числі приховано) технічні засоби, призначені для несанкціонованого втручання в роботу комп'ютерів, інформаційних систем, комп'ютерних мереж чи мереж електрозв'язку Банку, у тому числі комп'ютерні віруси та програмні закладки (шпигунське програмне забезпечення).
2.6.10. Нехтувати правилами інформаційної безпеки, які можуть призвести до ураження комп'ютерів Зовнішньої сторони, які взаємодіють з Банком, комп'ютерними вірусами та шкідливими програмними засобами і, таким чином, вплинути на інформаційну безпеку Банку.
2.6.11. Передавати у мережах зв'язку та передачі даних, що не контролюються Банком (у тому числі із застосуванням сервісів Internet, електронної пошти, миттєвих повідомлень), ІзОД Банку, якщо на це Банком не надано санкцію, а само повідомлення не зашифровано криптографічними засобами відповідно до вимог Банку.
2.6.12. Якщо Зовнішній стороні надані засоби зв'язку або передачі даних (у тому числі сервіси Internet, електронної пошти, миттєвих повідомлень тощо), що використовуються від імені Банку з метою передачі інформації за його межі, **ЗАБОРОНЯЄТЬСЯ**:

- використовувати вищезазначені засоби з метою, що суперечить інтересам Банку, вимогам законодавства України, міжнародним законодавчим актам, які ратифіковано Україною, а також з метою заподіяння шкоди іншим особам у наслідок порушення їх прав, релігійних, етнічних, політичних переконань тощо;
- використовувати засоби, що підміняють або маскують мережеву адресу комп'ютера користувача (IP- та MAC адресу), поштову адресу, а також ім'я (ідентифікатор доступу) користувача, під яким його зареєстровано у комп'ютерній мережі Банку (т.зв. анонімайзери);
- не надавати доступ до засобів Internet та електронної пошти із застосуванням власного ідентифікатора доступу та пароля іншим особам, у тому числі шляхом створення спільних (shared) ресурсів;
- не використовувати засоби Internet та електронної пошти з комерційними цілями, з метою реклами, агітації тощо, у тому числі не створювати засоби публікації в Internet (FTP, WWW-сторінки, електроні дошки об'яв), якщо це не пов'язано з виробничою діяльністю Банку;
- не розсилати поштові повідомлення будь-якого розміру або змісту, отримання яких не санкціоновано адресатами (spam), у тому числі рекламних та інформаційних об'яв на велику кількість адрес;
- не використовувати засоби Internet для отримання програмного забезпечення та даних з ненадійних джерел, а також у спосіб, що порушує авторське право та ліцензійні умови щодо їх розповсюдження;
- не використовувати криптографічні методи для приховування змісту повідомлень, що передаються, та методи стеганографії для приховування самого факту передачі, якщо ці дії не санкціоновано Банком;
- під час роботи в середовищі Internet не використовувати технічні засоби, призначені для збору та передачі медіа інформації (WEB-камери, мікрофони тощо), якщо такі дії не санкціоновано Банком.

3. Права представника Зовнішньої сторони
Представник Зовнішньої сторони, якого залучено до виконання робіт на підставі договорів цивільно-правового (господарського) характеру, укладених між Банком та Зовнішньою стороною, має право:

- бути ознайомленим з вимогами ІБ, визначені Договором, що його стосуються;
- бути ознайомленим з вимогами договору про конфіденційність, в частині, що його стосуються;
- бути ознайомленим з вимогами ІБ, правилами внутрішнього розпорядку та режиму безпеки Банку в частині, що його стосуються, а також зі змістом цих Інструктивних матеріалів;
- бути ознайомленим з переліком, методами та регламентом доступу до інформаційних ресурсів Банку, до яких представнику Зовнішньої сторони надається доступ;
- отримати відомості щодо порядку здійснення комунікацій з Банком у випадку виникнення інцидентів ІБ та надзвичайних ситуацій.