Міністерство охорони здоров'я України
Проєкт «Зміцнення системи охорони здоров'я та збереження життя»
№ 9468-UA

ЗАПИТ ДО ПОДАННЯ ЦІНОВИХ ПРОПОЗИЦІЙ
за пакетом № HEAL-RFQ-4.1.1.3
«Закупівля сукупності автоматизованих фільтрів (Web application firewall)»

1. Україна одержала позику Міжнародного банку реконструкції та розвитку (далі - Банк) 9468-UA на фінансування Проєкт «Зміцнення системи охорони здоров'я та збереження життя» (далі - Проект). Частина коштів цієї Позики має бути використана для покриття витрат в рамках договору, до якого відноситься цей запит до подання цінових пропозицій (далі – Запит).

2. Міністерство охорони здоров'я України (далі - Замовник) цим листом запрошує правомочних учасників торгів (тобто учасників, товари та/або програмне забезпечення, які вони пропонують, не підпадають під обмежувальні заходи (санкції) введені відповідно до чинних Указів Президента України) надіслати цінові пропозиції щодо постачання наступних товарів: комплект сукупності автоматизованих фільтрів (Web application firewall).

   Інформація щодо Технічних вимог та необхідних кількостей вказана в Додатках.

3. Учасник подає лише одну цінову пропозицію. Всі пропозиції учасника, який надав більше одної цінової пропозиції, будуть відхилені. Пропозиції мають бути повними (включати усі позиції) відповідно до цього Запиту. Неповні пропозиції будуть відхилені. Цінові пропозиції оцінюватимуться за всіма позиціями та договір буде присуджено фірмі, яка запропонувала найменшу оцінену вартість всіх позицій та відповідає усім умовам, встановленим цим Запитом та Технічними вимогами до нього.

4. Цінова пропозиція українською мовою за формою, наведеною у Додатку 3 «Цінова пропозиція» в сканованому вигляді разом з додатковою інформацією мають надсилатися за наступною електронною адресою:

   Міністерство охорони здоров'я України
   Офіс Групи консультаційної підтримки Проекту (ГКПП)
   Ел. пошта: moz.wb.procurement@gmail.com, **обов'язкова копія** на m.k.dymytrenko@moz.gov.ua. В полі «Тема» ел. повідомлення **обов'язково зазначити «Пакет № HEAL-RFQ-4.1.1.3».**
   Також за зверненням за вищевказаною адресою зацікавленими учасниками може бути отримана довідкова інформація.

5. Кінцевим терміном для отримання пропозицій Замовником за адресою вказаною в п. 4 вище встановлюється: **22 січня 2024 року, до 17:00 за місцевим часом**.

6. До своїх пропозицій Ви маєте додати відповідну документацію, що вимагається Технічними вимогами.

7. Процедура закупівлі – Запит до подання цінових пропозицій відповідно до вимог Правил закупівель Світового банку для позичальників в рамках фінансування інвестиційних проектів (ФІП), що опубліковані у липні 2016 року (переглянуті у листопаді 2017 року, серпні 2018 року та листопаді 2020 року).

Будь ласка, надайте Ваші цінові пропозиції відповідно до інструкцій у Запиті та Договору, що додається. «Умови надання послуг» та «Технічні вимоги», що додаються, є складовою частиною Договору.

(i) ЦІНИ. Ціни мають бути виражені в будь-якій валюті, включати ціну товарів у Місцях призначення, вказаних у Додатку 1 «Умови постачання», та включати усі обов'язкові платежі (податки, мито, тощо), та вартість додаткових та інших послуг, як зазначено у вищезгаданому Додатку.

(ii) ОЦІНКА ПРОПОЗИЦІЙ. Пропозиції, які визнані такими, що задовольняють Технічним вимогам та Запиту, оцінюватимуться шляхом порівняння загальної ціни відповідно до встановлених вимог, як вказано в п. (i) вище. У випадку подання цінових пропозицій у іншій валюті, з метою порівняння, Замовник конвертує всі ціни у валюту країни Замовника (українська гривня) по обмінному курсу продажу, опублікованому Національним банком України (https://bank.gov.ua/ua/markets/exchangerates) на дату кінцевого терміну отримання пропозицій, встановленого в п. 5 даного Запиту.

При оцінці пропозицій, Замовник визначить для кожної цінової пропозиції оціночну вартість шляхом коригування цінової пропозиції з метою виправлення арифметичних помилок таким чином:

а) якщо у будь-якому місці є невідповідність між сумою цифрами та прописом, сума прописом буде вважатися вірною;

б) якщо у будь-якому місці є невідповідність між ціною за одиницю та загальною сумою, яка обчислюється шляхом перемноження ціни за одиницю на кількість, ціна за одиницю буде вважатися вірною;

в) якщо Постачальник відмовиться прийняти вказані корегування, його цінова пропозиція буде відхилена.

(iii) ПРИСУДЖЕННЯ ДОГОВОРУ. Договір присуджуватиметься учаснику, який запропонує найнижчу загальну ціну, та пропозиція якого відповідає умовам, встановленими Технічними вимогами та Запитом. З обраним Постачальником буде укладено договір за формою, наведеною у Додатку 4 «Договір».

(iv) ТЕРМІН ЧИННОСТІ ПРОПОЗИЦІЙ: запропоновані цінові пропозиції повинні бути чинними протягом 45 (сорока п'яти) календарних днів від дати кінцевого терміну отримання пропозицій, встановленої в п. 5 даного Запиту.

8. **ПЕРЕВІРКИ ТА АУДИТ**

Постачальник повинен виконувати всі вказівки Замовника, які відповідають застосованому законодавству країни Замовника.

Постачальник повинен дозволяти, та забезпечити дозвіл всіх своїх підрядників та консультантів, на перевірку Банком та/або особами призначеними Банком всіх офісів Постачальника та всіх рахунків та документів, пов'язаних з впровадженням Договору та підготовкою цінової пропозиції, та дозволяти перевірку цих рахунків та документів аудитором, призначеним Банком, якщо це вимагатиме Банк. Увага Постачальника та його підрядників та консультантів звертається на статтю 5 «Шахрайство та корупція» Форми Договору, яка передбачає, серед іншого, що дії спрямовані на суттєве перешкоджання реалізації Банком його прав щодо перевірок та аудиту, становлять заборонену практику, яка може бути підставою для розірвання Договору (а також визнання Постачальника неправомочним відповідно до процедур Світового Банку щодо застосування санкцій).

9. **Будь ласка, надайте письмове підтвердження (електронною поштою) отримання цього Запиту та Вашої участі у торгах.**

Додатки:

Додаток 1. Умови надання послуг
Додаток 2. Технічні вимоги
Додаток 3. Цінова пропозиція
Додаток 4. Договір

ДОДАТОК 1

до Запрошення до подання цінових пропозицій № HEAL-RFQ-4.1.1.3

УМОВИ ПОСТАЧАННЯ

Назва пакету: «Закупівля сукупності автоматизованих фільтрів (Web application firewall)»
Номер пакету: HEAL-RFQ-4.1.1.3
Покупець: Міністерство охорони здоров'я України

1. Ціна пропозиції

№	Опис	Кільк., шт.	Ціна за одиницю [вказати валюту], включаючи усі податки, митні збори, доставку, завантаження, розвантаження, додаткові послуги без ПДВ	Загальна ціна [вказати валюту], без ПДВ
1	Комплект сукупності автоматизованих фільтрів (Web application firewall) [вказати виробника, модель]	*		
2				
ЗАГАЛЬНА ЦІНА **ПРОПОЗИЦІЇ** БЕЗ ПДВ				
ПДВ				
ЗАГАЛЬНА ЦІНА **ПРОПОЗИЦІЇ** З ПДВ				

***** *Кількість в комплекті залежить від виробника продуктів, які будуть задовольняти Технічним вимоги зазначеним у Додатку 2.*

Примітка 1: у разі розбіжності між сумою, підрахованою шляхом перемноження ціни за одиницю на кількість, та загальною ціною, підрахованою учасником торгів, чинною вважається загальна ціна, вирахувана на основі цін за одиницю.

2. Термін чинності цінової пропозиції

Запропонована цінова пропозиція є чинною протягом сорока п'яти (45) днів від дати кінцевого терміну отримання пропозицій, встановленої в п. 5 Запрошення до подання цінових пропозицій.

3. Фіксована ціна

Наведені вище ціни є фіксованими, включають усі податки, митні збори, доставку, завантаження, розвантаження, додаткові послуги до Місць призначення, вказаних у Додатку 1 «Умови постачання», і жодним змінам не підлягають, включаючи період виконання Договору.

4. Право Покупця змінювати кількість товарів під час присудження Договору

Покупець залишає за собою право під час присудження Договору збільшувати або зменшувати на 1-15% кількість товарів, визначених у «Запрошенні до подання цінових пропозицій» за умови, що не вноситься будь-яких змін до одиничних цін та інших умов постачання товарів.

5. Терміни та умови постачання

Постачання товарів разом із відповідними документацією та інструкціями з експлуатації та додатковими послугами (згідно з Технічними Вимогами, що додаються) має бути здійснено протягом 60 (шістдесяти) календарних днів від дати підписання Договору.
Постачальник може здійснювати поставку Товарів частинами, але не більше двох (2) поставок.

6. Оплата

Сто відсотків (100%) загальної ціни поставлених Товарів послуг буде сплачено Покупцем Постачальнику протягом тридцяти (30) календарних днів після виконання Постачальником всіх зобов'язань за Договором, окрім гарантійних зобов'язань, як зазначено у Додатку №1, підписання видаткової накладної між Покупцем та Постачальником та надання Постачальником наступних документів:

- оригіналів належним чином оформлених довіреностей на отримання Товарів, виписаних на матеріально відповідальних осіб у Місцях призначення;
- оригіналів видаткових накладних, виданих Покупцем, із підписами матеріально відповідальних осіб у Місцях призначення, на яких виписано довіреності на отримання Товарів;
- копії товарно-транспортних накладних Постачальника до Місць призначення;
- оригіналу рахунка-фактури Постачальника.

Видаткова накладна між Покупцем та Постачальником повинна бути підписана Покупцем протягом 5 днів з моменту отримання Покупцем вказаних в цьому пункті документів, або Покупець повинен надати Постачальнику письмову мотивовану відмову від підписання видаткової накладної.

Використання факсиміле при оформленні вищезазначених документів не дозволяється.

У разі відмінності валюти цінової пропозиції від української гривні – оплата буде здійснюватися в українській гривні за офіційним курсом Національного банку України на день підписання Покупцем видаткової накладної.

7. Гарантійні зобов'язання

Поставлені товари повинні мати гарантію Постачальника не менше, ніж строк, передбачений у Додатку № 2 «Технічні вимоги». Постачальник надає Покупцю гарантійні документи на товари разом з рахунком до сплати та видатковою накладною.
Протягом гарантійного періоду усі дефекти мають бути виправлені Постачальником без жодних витрат для Покупця не пізніше ніж через 30 днів з дати отримання повідомлення від Покупця.

8. Наслідки невиконання договору Постачальником

Покупець має право розірвати Договір без будь-яких зобов'язань перед Постачальником в разі невиконання поставки Товарів згідно наведених умов через 21 день після відповідного письмового повідомлення Покупцем.
За порушення строків поставки Товарів з Постачальника стягується неустойка у розмірі 0,2% від вартості Товарів, щодо яких допущено прострочення, за кожен календарний день прострочення. Неустойка, що стягується, не має перевищувати 10% вартості недопоставлених у строк Товарів.

9. Технічні вимоги

Наведені у Додатку 2 до Запрошення до подання цінових пропозицій. Постачальник має підтвердити відповідність запропонованих товарів специфікаціям по кожній позиції або навести усі розбіжності.

10. Інструкції з пакування та маркування

Постачальник має виконати стандартне пакування Товарів як вимагається для запобігання їх пошкодження чи порчі протягом транспортування до місця призначення як це вказано у Договорі.

11. Дефекти та недоліки

Усі дефекти та недоліки має бути виправлено Постачальником без будь-яких витрат з боку Покупця протягом 30 днів з дати повідомлення Покупцем про них.

[НАЗВА ВИКОНАВЦЯ]
Підпис уповноваженої особи:
Печатка компанії
Місце:
Дата:

[Примітка: Будь ласка ПІДПИШІТЬ та поставте ПЕЧАТКУ на ВСІ сторінки цього документу.]

ДОДАТОК А

до ДОДАТКУ 1

до Запрошення до подання цінових пропозицій № HEAL-RFQ-4.1.1.3

Вимоги до доставки Товарів до Місць призначення

Постачальник зобов’язаний забезпечити доставку (включаючи завантаження та розвантаження) кожної позиції Товарів до Місць призначень, зазначених у таблиці нижче.

№ п/п	Назва закладу	Адреса закладу
1.	Національна служба здоров'я України	04073, м. Київ, пр-т Степана Бандери, 19

ДОДАТОК 2

до Запрошення до подання цінових пропозицій № HEAL-RFQ-4.1.1.3

ТЕХНІЧНІ ВИМОГИ

Назва пакету:	«Закупівля сукупності автоматизованих фільтрів (Web application firewall)»
Номер пакету:	HEAL-4.1.1.3
Замовник:	Міністерство охорони здоров'я України

1. Загальні відомості

1.1 Загальні положення

У цьому документі наведені технічні вимоги до Web Application Firewall - Сукупність автоматизованих фільтрів для впровадження в ЦБД в т.ч. НСЗУ.

1.2 Призначення

WAF, призначений для виявлення та блокування сучасних атак на вебзастосунки інформаційних систем НСЗУ (ІС НСЗУ).

1.3 Мета проекту

Головною метою проекту є впровадження системи виявлення та блокування сучасних атак на вебзастосунки ІС НСЗУ.

Для доступу з мережі Інтернет доступні більше двадцяти вебзастосунків – Веб-сайти та публічні API. На вказані вебзастосунки постійно здійснюються проби кібератак з метою отримання несанкціонованого доступу до внутрішніх ресурсів ІС. НСЗУ, а також з метою завдання шкоди працездатності вебзастосунків.

Вже використовується для захисту вебзастосунків ІС НСЗУ хмарний сервіс захисту Cloudflare, який не має достатніх функціональних можливостей для захисту вебзастосунків всередині мереж ІС НСЗУ. Тому необхідна система захисту вебзастосунків від кібератак - фаєрвол веб-додатків (далі - WAF) розташовується безпосередньо перед сервером, на якому встановлено вебзастосунок. WAF буде аналізувати вміст HTTP/HTTPS трафіку (запити та відповіді), що передається між клієнтом (зазвичай браузер) та застосунком, а також виявляти та запобігати кібератакам на вебзастосунок.

Інфраструктури ІС НСЗУ розташовані в географічно рознесених датацентрах – Infrastrucrure НСЗУ, Azure. Для кожного з датацентрів необхідно впроваджувати окремі WAF, які будуть керуватись з централізованої панелі управління.

1.4 Цілі проекту

Для досягнення мети проекту потрібно впровадити систему захисту вебзастосунків ІС НСЗУ згідно наступної специфікації:

- ПАК WAF з пропускною здатністю трафіку до 500 Мбіт/с з технічною підтримкою на 3 роки
- Підписка на автоматичне оновлення репутаційних загроз для ПАК WAF в режимі реального часу з технічною підтримкою на 3 роки
- Сервіс класифікації користувачів в режимі реального часу з технічною підтримкою на 3 роки
- SSL Accelerator Card – карта прискорення обробки SSL трафіку з технічною підтримкою на 3 роки
- Сервер керування ПАК WAF з технічною підтримкою на 3 роки
- Віртуальний програмний комплекс WAF для платформи Microsoft Azure з пропускною здатністю L7 HTTP трафіку до 500 Мбіт/с з технічною підтримкою на 3 роки

1.5 Очікуваний результат

Впроваджено та прийнято в експлуатацію сучасну надійну систему виявлення та блокування сучасних атак на вебзастосунки ІС. НСЗУ, що відповідає усім вимогам, викладеним у цьому документі.

2. Терміни, визначення та скорочення

2.1 Перелік термінів

2.1.1 **WAF**

Web Application Firewall - міжмережний екран вебзастосунків

2.1.2 **TLS**

Transport layer security - протокол шифрування, який забезпечує захист даних, що передаються по мережі

2.1.3 **URL**

Uniform Resource Locator - унікальна адреса веб ресурсу (сайту), яка зареєстрована в єдиній схемі адресації

2.1.4 **API**

Application Programming Interface – Прикладний програмний інрерфейс

2.1.5 **OWASP**

Open Web Application Security Project - відкритий проект по забезпеченню безпеки веб-додатків

2.1.6 **SSL**

Secure Sockets Layer - криптографічний протокол, який забезпечує встановлення безпечного з'єднання між клієнтом і сервером

2.1.7 **SOAP**

Simple Object Access Protocol - протокол обміну структурованими повідомленнями в розподілених обчислювальних системах

2.1.8 **ПАК**

Програмно-апаратний комплекс – інформаційно-комунікаційна система, яка складається з програмного забезпечення (програм) та апаратного забезпечення (комп'ютерів, серверів, свічів тощо), які спільно працюють для вирішення конкретної задачі або групи задач. ПАК може включати в себе різні компоненти, такі як операційні системи, програми для обробки даних, сенсори для збору інформації, пристрої для виведення результатів тощо.

3. Вимоги чинного законодавства

Виконання робіт з придбання та впровадження WAF в ІС НСЗУ повинно відповідати вимогам чинних нормативно-правових документів: законів України «Про інформацію», «Про захист інформації в автоматизованих системах», «Про запобігання корупції», «Про доступ до публічної інформації», «Про звернення громадян»; указам Президента України від 09.12.2000 № 1323/2000 «Про додаткові заходи щодо до безперешкодної діяльності засобів масової інформації, дальшого утвердження свободи слова в Україні», від 31.07.2000 № 928/2000 «Про заходи щодо розвитку національної складової глобальної інформаційної мережі Інтернет та забезпечення широкого доступу до цієї мережі в Україні», від 17.02.2001 №101/2001 «Про удосконалення діяльності органів виконавчої влади з питань інформування населення», від 01.08.2002 № 683/2002 «Про додаткові заходи щодо забезпечення відкритості у діяльності органів державної влади».

Постачальник надає Покупцю програмно-апаратні засоби та ліцензії на доступ та використання Програмного продукту, включаючи усі винаходи, проекти та марки, втілені у Програмному продукті.

Програмний продукт ліцензується на умовах використання на Об’єктах проекту. Права інтелектуальної власності залишаються у їх власників.

Ліцензії повинні:

(a) бути:
   i. невинятковими;
   ii. повністю оплаченими та безвідкличними;
   iii. враховувати спеціальні пільгові ціни на ліцензії, які певні виробники надають для державних установ в Україні;
   iv. без будь-яких часових обмежень щодо доступу та використання;
   v. дійсними на всій території країни Покупця.

(b) забезпечувати стосовно Програмного продукту:
   i. можливість ним користуватися та робити копії для використання на (або з) комп’ютером (комп’ютерами), для якого його придбали, плюс на резервному комп’ютері (комп’ютерах) такої ж або аналогічної потужності, якщо основний (основні) знаходиться в неробочому стані та під час обґрунтовано необхідного перехідного періоду при переході з основного на резервний комп’ютер;
   ii. його використання або копіювання для використання на (або для) передачі на запасний комп’ютер (комп’ютери), (та використання на первинному та запасному комп’ютері (комп’ютерах) може здійснюватися одночасно під час обґрунтовано необхідного перехідного періоду).

Програмний продукт, що постачається та його складові частини, не повинні мати статус **EOL/EOS** (End-of-Life/End-of-Support) на момент подачі пропозицій постачальника.

Ліцензії на програмний продукт (далі ПП) включають технічну підтримку програмного забезпечення не менш ніж строк дії ліцензії з фактичної дати поставки.

4. Вимоги до WAF НСЗУ

Загальні вимоги

- WAF повинен поставлятися у форматі програмного-апаратного комплексу у вигляді віртуальних машин та фізичних серверів.
- Повинна підтримуватись платформа віртуалізації VMware хмарні платформи Microsoft Azure та Amazon Web Services.
- Фізичні сервери повинні мати карти прискорення обробки TLS трафіку.
- Рішення повинно мати централізоване управління

4.1.Функціональні вимоги WAF в НСЗУ

4.1.1. WAF має підтримувати як позитивну, так і негативну моделі безпеки.

a. Негативна модель безпеки визначатиме відомі сигнатури атак.
   i. Транзакції, вміст яких збігається із відомими сигнатурами атак, блокуються. Решту дозволено.
   ii. Негативна модель безпеки повинна включати попередньо налаштований всеосяжний і точний список атак сигнатур.
   iii. WAF повинен дозволяти модифікацію або додавання сигнатур.
   iv. WAF повинен підтримувати автоматичне оновлення списку сигнатур, забезпечуючи повний захист від нових загроз.
   v. Негативна модель безпеки повинна дозволяти виявляти відомі атаки на кількох рівнях, у тому числі на рівні мережі, операційної системи, програмного забезпечення веб-сервера та атак на рівні програм.

b. Позитивна модель безпеки передбачає, що дозволено все, що відомо, а решта блокується.
   i. Позитивна модель безпеки повинна включати URL-адреси, каталоги, cookie, поля форм з параметрами і методи HTTP.
   ii. З метою зниження трудомісткості налаштування позитивної моделі безпеки, WAF повинен мати механізм автоматичного вивчення та оновлення структури веб-додатку та його елементів.

4.1.2. Перебуваючи в режимі навчання протягом обмеженого періоду часу, WAF запам'ятовує параметри, що вводяться легітимними користувачами в різні поля форм веб-програми.

4.1.3. WAF повинен забезпечувати безперервне автоматичне вивчення шаблону нормальної роботи веб-програми з урахуванням можливих запланованих змін структури та даних веб-програми, і той самий час забезпечувати активне блокування відхилень від норми:

a. Прийнятні значення параметрів полів форм запису в профіль.
b. Записані значення параметрів використовуються як критерії перевірки легітимності запитів у позитивній моделі безпеки.
c. Режим навчання служить для створення моделі структури та елементів програми (каталогів, URL-сторінок, параметрів, cookie) та очікуваної поведінки користувача (очікувані діапазон зміни значень параметрів, прийнятні символи, чи призначений параметр для читання чи редагування

клієнтом, чи є він обов'язковим чи опціональним). Все це допомагає автоматизувати налаштування позитивної моделі безпеки.

d. Передбачена можливість зміни конфігурації профілю вручну адміністратором.
e. Механізм автоматичної побудови моделі програми (навчання) виявляє вузькі місця у профілі та пропонує відповідні заходи (зміни) для його оптимізації, наприклад, перетворення URL на параметри та ін.
f. Повинен бути передбачений механізм автоматичного переведення на повторне навчання.

4.1.4. WAF повинен виявляти відомі шкідливі джерела автоматизованих атак та атак з використанням ботнетів, анонімних проксі, мереж TOR, фішингових сайтів.

4.1.5. WAF повинен вміти відстежувати вдалі входи користувачів до веб-додатків та збагачувати події безпеки відповідною інформацією.

4.1.6. WAF повинен забезпечувати можливість створення складних безпекових політик, що використовують у тому числі дані зовнішніх систем (наприклад, Active Directory) за допомогою інтуїтивно зрозумілого графічного інтерфейсу, не вимагаючи застосування будь-якої мови програмування.

4.1.7. WAF повинен виявляти та дозволяти/блокувати запити користувачів за географічною ознакою.

4.1.8. WAF повинен забезпечувати захист програмних інтерфейсів додатків (Application programming interfaces, API).

4.1.9. WAF має відрізняти ботів від користувачів та мати можливість захищати веб-додатки за допомогою CAPTCHA.

4.1.10. WAF має вміти корелювати події безпеки, щоб відрізняти легітимні запити від шкідливих.

4.1.11. WAF повинен підтримувати правила користувача (політики) безпеки. Адміністратори повинні мати можливість створювати політики як для позитивної, так і для негативної моделі безпеки, а також створювати кореляційні правила, що містять декілька критеріїв.

4.1.12. При розгортанні як проксі (прозорий або зворотний проксі) WAF повинен підтримувати цифровий підпис cookie, шифрування cookie і перезапис URL.

4.1.13. WAF повинен володіти інтерфейсом інтеграції зі сканерами вразливостей.

4.1.14. WAF повинен мати можливість інтеграції із системами управління подіями безпеки SIEM.

4.1.15. WAF повинен усувати більшість із перелічених у списку OWASP Top 10 вразливостей веб-застосунків. Перелік загроз OWASP Top 10 викладено у розділі «Список OWASP Top 10» цього документа.

4.2.Вимоги щодо розгортання та використання WAF в НСЗУ

4.2.1 WAF повинен мати можливість розгортання у варіанті in-line як прозорий міст, зворотний або прозорий проксі-сервер. WAF також повинен бути готовим до розгортання в режимі off-line як сніфер (пасивний мережевий монітор).

4.2.2 WAF повинен підтримувати пасивний та активний режими роботи:

a. У пасивному режимі WAF дозволяє адміністратору переглядати повідомлення про атаки, про помилки роботи сервера, про інші несанкціоновані дії.
b. В активному режимі WAF повинен мати можливість блокування атак.
c. При виявленні атаки або будь-яких несанкціонованих дій WAF має бути в змозі вжити відповідних заходів. Дії, що підтримуються, повинні включати можливість скидати конкретні запити та відповіді, блокувати цілі сесії, запити від конкретних користувачів додатків або з певних IP-адрес. Для особливо небезпечних атак WAF повинен вміти блокувати всі запити від конкретного користувача або з конкретної IP-адреси за певний період часу.
d. У режимі пасивного мережевого моніторингу (сніфера) WAF повинен мати можливість відправляти пакет TCP RST серверу додатків. Крім того, WAF у режимі моніторингу може повідомляти про аномальну поведінку, але не робити жодних дій у відповідь.

4.2.3 WAF повинен мати лінійну пропускну здатність і латентність у декілька мілісекунд, щоб не впливати на продуктивність веб-додатків.

4.2.4 WAF повинен мати можливість працювати з HTTP і HTTPS (SSL) трафіком веб-додатків.

4.2.5 Для захисту SSL веб-застосунків повинна бути передбачена можливість імпорту до WAF сертифікатів і пар закритий/відкритий ключ веб-серверів.

4.2.6 Для захисту SSL веб-додатків WAF термінуватиме та розшифровуватиме клієнтські з'єднання, перевірятиме трафік на предмет відповідності політикам безпеки та, залежно від режиму, може повторно його зашифровувати при з'єднаннях із веб-серверами.

4.2.7 У режимах мосту і сніфера WAF повинен вміти розшифрувати трафік SSL для перевірки, не термінуючи або змінюючи HTTPS з'єднання.

4.2.8 WAF повинен бути здатний захищати веб-програми, які містять XML контент. Захист XML повинен бути еквівалентним захисту веб-додатків з використанням механізму автоматизованого навчання (профілювання).

4.2.9 WAF має підтримувати можливість роботи в режимі високої доступності (High availability).

4.3.Вимоги до моніторингу та звітності

4.3.1 WAF повинен підтримувати:

a. Перевірку та контроль HTTP трафік, включаючи HTTP заголовки, поля форм, а також дані, що передаються.
b. Перевірку HTTP запитів та відповідей.
c. Декодування даних для подання у текстовому вигляді з метою подальшої перевірки.

d. Перевірку для URL, форм, cookie , рядків запиту, прихованих полів та параметрів, методів HTTP, XML елементів та SOAP дій.

4.3.2 WAF повинен підтримувати належну звітність та можливість журналювання:

a. Має можливість формування звіту про події за допомогою стандартних механізмів, наприклад, у системний журнал.
b. Рівні ведення журналу та фільтри повинні встановлюватися адміністратором.
c. WAF повинен мати можливість формувати табличні та графічні звіти, мати готові шаблони звітності
d. Ці звіти мають бути доступні як на вимогу, так і за розкладом і розповсюджуватися за протоколом SMTP.
e. Інтерфейс керування WAF повинен мати графічну панель, що інформує про його стан та веб-активність.

4.3.3 WAF повинен мати можливість ідентифікувати користувачів веб-програми. Механізм ідентифікації користувачів повинен бути автоматизованим, не передбачати внесення будь-яких змін до існуючої програми або схеми автентифікації програми.

4.4.Вимоги до архітектури впровадження

WAF має підтримувати такі варіанти розгортання: Reverse Proxy , Transparent Bridge та Sniffer.

4.4.1 Режим зворотного проксі-сервера

У даній топології WAF має діяти як Reverse Proxy та термінувати HTTP/HTTPS з'єднання. При цьому Reverse Proxy повинен розташовуватися між веб-серверами та користувачами, здійснюючи статичне перетворення внутрішньої адреси веб-сервера на зовнішній, за яким користувачі звертаються до нього. У випадку, коли WAF розгорнуто як зворотний проксі, необхідна переконфігурація мережі:

- Коригування записів у DNS – ті, що спочатку вказували на IP-адреси веб-сервера повинні вказувати на IP-адреси WAF.
- Налаштування міжмережевих екранів таким чином, щоб заборонити безпосередній доступ до IP-адрес веб-серверів.
- Відповідне налаштування маршрутизації.

4.4.2 Режим прозорого мосту

У цій топології WAF повинен діяти як прозорий міст і не термінує HTTP/HTTPS з'єднання. Весь трафік до веб-серверів, що захищаються, повинен пройти через WAF (перехоплюється і обробляється WAF). WAF перевіряє трафік та блокує шкідливий трафік. Решта трафік проходить крізь WAF без перевірки (прозоро).

4.4.3 Режим пасивного моніторингу мережі

У цій топології WAF має бути підключений до SPAN порту комутатора або до пристрою Tap Ethernet. Веб-трафік не проходить через WAF, а надходить на його порти, що прослуховують. У цій топології WAF повинен пасивно відстежувати та сповіщати про події безпеки. При необхідності, у разі виявлення порушень правил захисту - скидати сесію TCP шляхом відправки команди TCP Reset серверу.

4.5.Список OWASP «Top 10»

Open Web Application Security (OWASP) є відкритим проектом, який розробив документацію та інструменти, щоб допомогти користувачам захистити свої веб-програми та відповідні служби. Метою проекту OWASP «Top 10» (список десяти найуразливіших веб-додатків, що найчастіше зустрічаються) є збільшення поінформованості про безпеку веб-додатків за допомогою визначення найбільш критичних ризиків, що загрожують організаціям. На проект " Top 10" посилається безліч стандартів, інструментів та організацій, включаючи MITRE, PCI DSS, DISA, FTC та багато інших.

4.6. Список OWASP десяти найуразливіших веб-додатків, що найчастіше зустрічаються:

1) A1:2017-Injection
2) A2:2017-Broken Authentication
3) A3:2017-Sensitive Data Exposure
4) A4:2017-XML External Entities (XXE)
5) A5:2017-Broken Access Control
6) A6:2017-Security Misconfiguration
7) A7:2017-Cross-Site Scripting (XSS)
8) A8:2017-Insecure Deserialization
9) A9:2017-Using Components with Known Vulnerabilities
10) A10:2017-Insufficient Logging&Monitoring

WAF повинен виявляти та блокувати атаки на перераховані вище вразливості.

5. Вимоги до якості послуг

Послуги мають надаватись за встановленими показниками якості відповідно до діючих в Україні державних стандартів, технічних умов, нормативно-правових актів, інших нормативно-технічних документів, які встановлюють вимоги до показників якості такого роду/виду послуг, а також відповідно до наданої Замовником Виконавцю інформації про умови надання послуг.

Для підтвердження законності надання запропонованих послуг на території України учасник повинен надати лист в довільній формі від компанії-виробника адресоване на ім'я Замовника та з посиланням на дану процедуру закупівлі. В листі обов'язково повинно бути зазначено про права учасника здійснювати продаж продуктів (сервісів) виробника на території України

Контроль за якістю надання послуг повинен здійснюватися із залученням уповноваженого представника НСЗУ протягом всього періоду їх надання.

6. Вимоги до гарантійного обслуговування

Термін гарантійного обслуговування повинен складати не менше 12 календарних місяців із дати закінчення договору.

Замовник інформує Виконавця стосовно проблем, що виникають в процесі експлуатації ПЗ шляхом надсилання електронного листа на адресу Виконавця (далі - Заявка).

У разі виникнення збоїв, що унеможливлюють подальшу роботу WAF, Замовник інформує Виконавця або відповідальних представників Виконавця в телефонному режимі з подальшим створенням Заявки.

За запитом Виконавця Замовник оперативно надає додаткову інформацію, необхідну для надання Послуг.

Заявка повинна містити максимально розширений опис помилки, а також при можливості іншу інформацію, потрібну для надання Послуг.

Вимоги до часу реакції на звернення Замовника:

уповноважені працівники Замовника, проаналізувавши технічну проблему та прийнявши рішення щодо необхідності залучення Виконавця, присвоюють зазначеній технічній проблемі категорію:

критично – проблема призводить до непрацездатності або перебоїв у роботі всієї Системи, чи окремого модулю, або до неможливості використання модулю користувачами;

терміново – проблема призводить до збою роботи однієї із функцій WAF;

не терміново – проблема призводить до помилок у програмному забезпеченні, що не увійшли у категорію «критично» чи «терміново».

Несправністю WAF називається неналежне його функціонування.

Помилкою у документації називається невідповідність опису роботи функціоналу WAF у керівництвах з інсталяції, керівництвах користувачів, адміністраторів.

Несправностями не визнаються будь-які помилки в програмному забезпеченні і обладнанні третіх осіб, що використовуються Замовником при експлуатації WAF.

Виконавець, у відповідь на запит, повинен розпочати вирішення технічної проблеми в залежності від присвоєної категорії:

критично – усунення інциденту протягом 16 робочих годин з моменту надходження заявки. Усунення помилки протягом 4 робочих днів з моменту надходження заявки (включаючи установку і перевірку у замовника);

терміново – протягом 5 робочих днів з моменту надходження заявки (включаючи установку і перевірку у замовника);

не терміново – протягом 10 робочих днів або по узгодженню з Замовником (включаючи установку і перевірку у замовника) з моменту надходження заявки.

7. Вимоги чинного законодавства

Розгортання та впровадження WAF в НСЗУ повинно відповідати вимогам чинних нормативно-правових документів, а саме:

- Закону України «Про інформацію»;
- Закону України «Про електронні документи та електронний документообіг»;
- Закону України «Про звернення громадян»;
- Закону України «Про захист інформації в інформаційно-комунікаційних системах»;
- Закону України «Про електронні довірчі послуги»;
- Закону України «Про захист персональних даних»;

- Закону України «Про доступ до публічної інформації»;
- постанові Кабінету Міністрів України від 29.03.2006 № 373 «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах»;
- постанові Кабінету Міністрів України від 04.02.1998 № 121 «Про затвердження переліку обов'язкових етапів робіт під час проектування, впровадження та експлуатації засобів інформатизації»;
- ДСТУ ISO/IEC/IEEE 12207:2018. Інженерія систем і програмних засобів. Процеси життєвого циклу програмних засобів;
- ДСТУ ISO/IEC/IEEE 15288:2016 Інженерія систем і програмного забезпечення. Процеси життєвого циклу систем (ISO/IEC/IEEE 15288:2015, IDT);
- ДСТУ ISO/IEC 2382:2017 (ISO/IEC 2382:2015, IDT). Інформаційні технології. Словник термінів;
- ДСТУ ISO/IEC 14764:2014. Інженерія програмного забезпечення. Процеси життєвого цик-лу програмного забезпечення. Технічне обслуговування;
- ДСТУ 4163:2020. Державна уніфікована система документації. Уніфікована система організаційно-розпорядчої документації. Вимоги до оформлення документів;
- ДСТУ 3008:2015 Інформація та документація. Звіти у сфері науки і техніки. Структура та правила оформлювання;
- НД ТЗІ 1.1-003-99. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу;
- НД ТЗІ 2.5-005-99. Класифікація автоматизованих систем і стандартні функціональні про-філі захищеності оброблюваної інформації від несанкціонованого доступу;
- ДСТУ 2226-93 Автоматизовані системи. Терміни та визначення;

8. Графік впровадження

№	Склад і зміст робіт	Орієнтовний Термін розробки (в робочих днях*)	Дата здачі роботи
1	Розробка технічного завдання (ТЗ) та календарного плану робіт, в тому числі: 1.1. Провести аналіз інформації, інформаційних систем та комплексів, що використовуються на даний час, визначити Цільову аудиторію, визначити потреби Замовника. 1.2. Сформувати деталізовані вимоги до WAF НСЗУ в виді документу «Технічне завдання на впровадження WAF».	15	

2	Встановлення ПАК WAF	5	
3	Встановлення та налаштування автоматичного оновлення репутаційних загроз для ПАК WAF в режимі реального часу	10	
4	Встановлення та налаштування сервісу класифікації користувачів в режимі реального часу	10	
6	Встановлення та налаштування карти прискорення обробки SSL трафіку	5	
8	Встановлення та налаштування серверу керування ПАК WAF	5	
9	Встановлення та налаштування віртуального програмного комплексу WAF для платформи Microsoft Azure	5	
10	Проведення тестування програмного забезпечення в обсязі попередніх випробувань, в тому числі: 5.1. Підготовка проєкту «Програми та методики випробувань» 5.2. Розгортання та налаштування програмного забезпечення 5.3 Проведення ручного тестування згідно проекту «Програми та методики випробувань»	30	
11	Розробка технічної документації.	10	
12	Навчання персоналу Замовника.	30	
13	Приймання WAF та введення його в промислову експлуатацію	10	
14	Послуги з гарантійного обслуговування WAF ІС НСЗУ	12 міс.	

Приймання WAF та введення його в промислову експлуатацію (виконання етапу №13)

Постачальник має виконати приймальні випробування всього поставленого, встановленого та налаштованого програмного забезпечення з тим, щоб було забезпечено їх функціонування у відповідності до вимог, зазначених у цих Технічних специфікаціях.

Приймання WAF проводиться шляхом проведення приймальних випробувань. Приймальні випробування здійснюються приймальною комісією, в яку входять уповноважені представники Покупця, Постачальника та інші особи відповідно до вимог Договору.

Ціль приймальних випробувань полягає в підтвердженні і відповідності вимогам цих Технічних специфікацій.

Види, склад, обсяг і методи випробувань визначаються програмою приймальних випробувань. Програми приймальних випробувань розробляється Постачальником і узгоджується Покупцем не пізніше, ніж за 1 день перед початком випробувань.

При виявленні під час приймальних випробувань недоліків, дефектів або інших відхилень від вимог Технічних специфікацій, відповідні факти фіксуються в протоколі, в якому в тому числі вказується:

- перелік недоліків (дефектів);
- ступінь впливу зазначених недоліків на працездатність;
- необхідні терміни усунення недоліків (дефектів).

Протягом тридцяти робочих днів з моменту усунення недоліків, дефектів або інших відхилень від вимог приймальна комісія повинна провести повторні приймальні випробування.

Хід проведення приймально-здавальних випробувань Замовник та Виконавець документують у «Протоколі випробувань».

За результатами успішних випробувань та на підставі протоколу випробувань Виконавець спільно із Замовником підписують «Акт приймання-передачі WAF НСЗУ».

Постачальник повинен забезпечити Покупця документацією, використовуючи скріншоти, лістинги команд, схему мережі, яка відображає фізичні з’єднання із зазначенням використовуваних фізичних та логічних інтерфейсів – Технічний паспорт.

9. Вимоги до впровадження

9.1. Впровадження повинно виконуватись сертифікованим інженером. Інженер повинен мати можливість проводити офіційні вендорські або авторські навчальні курси по WAF, мати відповідну навчальну програму та лабораторію, надавати навчальні матеріали (Lab book).

9.2. Впровадження включає переключення під захист 20 веб-додатків.

9.3. Орієнтовний перелік робіт:

- Узгодження режиму застосування.
- Складання підготовчих вимог
- Надання образів та настановних пакетів
- Складання та узгодження плану робіт
- Розгортання шлюзів та сервера управління

- Початкова конфігурація віртуальних машин та фізичних серверів, налаштування доступу для підключення шлюзів до сервера управління
- Налаштування інтерфейсів та маршрутизації, відмовостійкості. Перевірка доступів
- Імпорт ліцензії
- Налаштування оновлень
- Встановлення актуальних патчів
- Інтеграція з AD
- Інтеграція з SMTP та/або SIEM
- Додавання адміністративних користувачів GUI сервера управління, розмежування доступу та привілеїв
- Налаштування режиму роботи шлюзів
- Створення дерева сайтів та сервісів
- Налаштування правил проксіювання або бриджування
- Налаштування роботи з шифрованим трафіком
- Тестова перевірка доступності сайтів, траблшутинг
- Налаштування Error page та Error page політик
- Тонка настройка сервісів (redirect, rewrite тощо)
- Створення логічних додатків та підпрограм, налаштування профілювання
- Створення додаткових механізмів безпеки та оповіщення
- Доналаштування out-of-box політик, створення користувачів
- Налаштування репутаційних сервісів
- Робота з false positives, додавання винятків, тюнінг політик
- Оптимізація профілів додатків
- Створення та налаштування звітності
- Переведення веб-додатків до активного блокування WAF.
- Налаштування нативного моніторингу системи
- Налаштування створення резервних копію конфігурації системи

9.4. Розробка технічної документації.

9.5. Навчання персоналу Замовника.

9.6. Приймальні випробування.

[НАЗВА ВИКОНАВЦЯ]
Підпис уповноваженої особи:
Печатка компанії
Місце:
Дата:

[Примітка: Будь ласка ПІДПИШІТЬ та поставте ПЕЧАТКУ на ВСІ сторінки цього документу.]

ДОДАТОК 3

до Запрошення до подання цінових пропозицій № HEAL-RFQ-4.1.1.3

[НА БЛАНКУ ОРГАНІЗАЦІЇ]

ЦІНОВА ПРОПОЗИЦІЯ

Міністерство охорони здоров'я України

01601, Україна, Київ,
вул. М. Грушевського, 7

Шановні панове,

Ми пропонуємо виконання договору № HEAL-RFQ-4.1.1.3 «Закупівля сукупності автоматизованих фільтрів (Web application firewall)» відповідно до «Умов постачання» та «Технічних вимог», які надаються разом із цією ціновою пропозицією, за ціною договору _____*(сума прописом і цифрами)* (_____) *(назва валюти)*. Ми пропонуємо завершити доставку Товарів, описаних в договорі в межах періоду в _____ календарних днів від дати підписання договору.

Ця цінова пропозиція і ваше письмове повідомлення про її прийняття становитимуть зобов'язання укласти з вами договір за формою, наведеною у Запрошенні до подання цінових пропозицій № HEAL-RFQ-4.1.1.3. Ми розуміємо, що ви не зобов'язані приймати цінову пропозицію з найнижчою ціною, або будь-яку іншу цінову пропозицію, отриману вами.

Цим документом ми підтверджуємо, що:

а) дана цінова пропозиція є дійсною протягом сорока п'яти (45) днів з кінцевої дати надання цінової пропозиції зазначеної у п.5 Запрошення до подання цінових пропозицій № HEAL-RFQ-4.1.1.3.

б) Постачальник та запропоновані ним товари та програмне забезпечення не підпадають під обмежувальні заходи (санкції) введені відповідно до чинних Указів Президента України.

_____ Дата: _____

[Підпис уповноваженої особи Постачальника] [День/Місяць/Рік]

П.І.Б. уповноваженої особи Постачальника: _____

Назва Постачальника: _____
Адреса: _____
_____
Тел. _____
Факс _____

Додаток 1: Умови постачання
Додаток 2: Технічні вимоги

[Примітка: Будь ласка ПІДПИШІТЬ та поставте ПЕЧАТКУ на ВСІ сторінки цього документу.]

ДОДАТОК 4

до Запрошення до подання цінових пропозицій № HEAL-RFQ-4.1.1

ДОГОВІР № HEAL-RFQ-4.1.1.3/___

м. Київ _____ 2023 р.

Цей Договір укладено в день, місяць та рік, зазначені вище, між Міністерством охорони здоров'я України (далі – Покупець), в особі _____, заступника Міністра охорони здоров'я України, яка діє на підставі наказу Міністерства охорони здоров'я України від _____ № _____, з однієї сторони, та _____ (далі - Постачальник) в особі _____, який діє на підставі Статуту, з іншої сторони, які надалі разом іменуються «Сторони», а кожен окремо «Сторона».

Договір укладається в рамках реалізації Проєкту "Зміцнення системи охорони здоров'я та збереження життя" (Heal Ukraine) (далі – Проєкт), що фінансується відповідно до Угоди про позику між Україною та Міжнародним банком реконструкції та розвитку (далі – Банк) від 22.12.2022 № 9468-UA (далі – Угода про позику).

1. ПРЕДМЕТ ДОГОВОРУ

1.1. Постачальник зобов'язується поставити Покупцеві комп'ютерну, офісну техніку та супутні товари (далі – Товари), а Покупець зобов'язується придбати (прийняти та оплатити) Товари на умовах даного Договору.
1.2. Вартість, асортимент, кількість та технічні специфікації Товарів вказуються в Додатку № 1 «Умови постачання» та Додатку № 2 «Технічні вимоги», які є невід'ємною частиною цього Договору.

2. ДОСТАВКА ТА ПРИЙМАННЯ

2.1. Постачальник здійснює поставку Товарів Покупцеві до Місць призначень та протягом термінів, зазначених в Додатку №1 до цього Договору. Постачальник може здійснювати поставку Товарів частинами, але не більше двох (2) поставок.

2.2. Датою поставки Товарів вважається дата підписання Сторонами видаткової накладної. Видаткова накладна повинна бути підписана Покупцем в день поставки Товарів або протягом цього дня Покупець повинен надати Постачальнику письмову мотивовану відмову від підписання видаткової накладної. Факт підписання Сторонами видаткової накладної визначає момент переходу права власності на Товари від Постачальника до Покупця.

3. СУМА ДОГОВОРУ та ОПЛАТА

3.1. Сума Договору складає _____ (_____), включаючи усі податки, митні збори, доставку, завантаження, розвантаження та додаткові послуги включно із ПДВ у сумі _____. Сума Договору та одиничні ціни Товарів, вказані в Додатку № 1, є фіксованими і змінам не підлягають.

3.2. Сто відсотків (100%) загальної ціни поставлених Товарів послуг буде сплачено Покупцем Постачальнику протягом тридцяти (30) календарних днів після виконання Постачальником всіх зобов'язань за Договором, окрім гарантійних зобов'язань, як зазначено у Додатку №1, підписання видаткової накладної між Покупцем та Постачальником та надання Постачальником наступних документів:

- оригіналів належним чином оформлених довіреностей на отримання Товарів, виписаних на матеріально відповідальних осіб у Місцях призначення;
- оригіналів видаткових накладних, виданих Покупцем, із підписами матеріально відповідальних осіб у Місцях призначення, на яких виписано довіреності на отримання Товарів;

- копії товарно-транспортних накладних Постачальника до Місць призначення;
- оригіналу рахунка-фактури Постачальника.

Видаткова накладна між Покупцем та Постачальником повинна бути підписана Покупцем протягом 5 днів з моменту отримання Покупцем вказаних в цьому пункті документів, або Покупець повинен надати Постачальнику письмову мотивовану відмову від підписання видаткової накладної.
Постачальник може здійснювати поставку Товарів частинами, але не більше двох (2) поставок.

3.3 Оплата за цим Договором здійснюється за рахунок коштів позики (Угода про позику між Україною та Міжнародним банком реконструкції та розвитку від 22.12.2022 № 9468-UA), передбачених у спеціальному фонді державного бюджету.

3.4 На період дії воєнного стану в Україні оплата здійснюється у порядку черговості відповідно до Порядку виконання повноважень Державною казначейською службою в особливому режимі в умовах воєнного стану, затвердженого постановою Кабінету Міністрів України від 09 червня 2021 року № 590.

4. ПРИПИНЕННЯ ДІЇ ДОГОВОРУ

4.1 Припинення дії у зв'язку з невиконанням договірних зобов'язань

(a) Покупець, без шкоди будь-яким іншим заходам, пов'язаним із порушенням умов Договору, може розірвати Договір цілком або частково, надіславши Постачальнику в письмовій формі повідомлення про невиконання останнім зобов'язань за Договором:

(i) у разі, якщо Постачальник неспроможний поставити будь-які або всі товари в межах періоду, визначеного в Договорі, або в межах будь-якого наданого його продовження;

(ii) у разі, якщо Постачальник неспроможний виконати будь-яке інше зобов'язання за Договором; або

(iii) у разі, якщо Постачальник, на думку Покупця, був замішаний у корупції або шахрайстві, як зазначено в п. 5 нижче в процесі конкуренції за отримання або виконання Договору.

(b) Якщо Покупець розриває Договір повністю або частково, Покупець може, на прийнятних умовах і в доцільний спосіб, закупити аналогічні недопоставлені Товари, причому Постачальник буде нести перед Покупцем відповідальність за всі додаткові витрати, пов’язані з такими аналогічними Товарами. Однак Постачальник повинен продовжувати виконання Договору в тій його частині, що не була розірвана.

4.2 Розірвання Договору в силу неплатоспроможності

(a) Покупець може в будь-який час розірвати Договір, направивши Постачальнику відповідне письмове повідомлення, якщо Постачальник стає банкрутом або в інший спосіб оголошується неплатоспроможним. В цьому випадку розірвання здійснюється без виплати компенсації Постачальнику за умови, що таке розірвання не шкодить або не впливає на будь-які права щодо дій або коригувальних заходів, що були чи будуть згодом набуті Покупцем.

4.3 Розірвання Договору в силу доцільності

(a) Покупець може в будь-який час повністю або частково розірвати Договір в силу доцільності, надіславши Постачальнику відповідне письмове повідомлення У цьому повідомленні повинно бути зазначено, що таке розірвання здійснюється з міркувань

доцільності для Покупця, визначено обсяг анульованих зобов'язань Постачальника за Договором, а також дату вступу в силу такого розірвання.

(b) Товари, вже готові до відправлення протягом двадцяти восьми (28) днів після одержання Постачальником повідомлення про розірвання, повинні бути прийняті Покупцем на умовах і за цінами Договору. По відношенню до інших Товарів Покупець може зробити наступний вибір:

(i) вимагати виготовлення і поставки будь-якої їхньої частини на умовах і за цінами Договору; та /або

(ii) відмовитися від Товарів.

5. ШАХРАЙСТВО ТА КОРУПЦІЯ

5.1 У разі, якщо Покупець виявить, що Постачальник та/або будь-хто з його працівників, агентів, субпідрядників, консультантів, надавачів послуг, постачальників та/або найманих працівників вдавались до корупційних або шахрайських дій, або до практики змови, примусу, перешкоджання розслідуванню в процесі конкурентного відбору або при виконанні цього Договору, у цьому випадку Покупець може припинити залучення Постачальника за Договором і дію Договору, письмово повідомивши про це Постачальника не пізніше, ніж за 14 днів до припинення дії Договору. При цьому положення пункту 4 застосовуються так ніби мало місце припинення дії Договору відповідно до пп.4.1.

5.2 Від Постачальника вимагається дотримання вимог Антикорупційного керівництва Банку та його переважаючих політик та процедур щодо санкцій, викладених в Санкційних правилах Банку, як визначено в Додатку 3 до Договору.

6. ПЕРЕВІРКИ ТА АУДИТ

6.1 Постачальник має виконувати всі вказівки Покупця, які відповідають чинному законодавству місця постачання товарів.

6.2 Постачальник дозволяє Банку і/або особам, призначеним Банком, а також має забезпечити отримання дозволу від своїх Субпідрядників та консультантів, інспектувати і/або проводити на вимогу Банку аудит рахунків, записів та інших документів, що мають відношення до подання тендерної пропозиції та виконання Договору. Звертаємо увагу Постачальника, його Субпідрядників та консультантів на п.5 Шахрайство та корупція, яким, окрім іншого, передбачається, що дії, спрямовані на суттєве обмеження реалізації Банком свого права на проведення перевірок та аудиту становить заборонену практику, яка тягне за собою розірвання договору і/або застосування Банком санкцій (включаючи визнання Постачальника неправомочним, але не обмежуючись цим) відповідно до стандартних процедур Банку щодо застосування санкцій.

7. ГАРАНТІЙНІ ЗОБОВ'ЯЗАННЯ

7.1. Товари повинні мати гарантію Постачальника не менше, ніж строк, передбачений у Додатку № 2 «Технічні вимоги». Постачальник надає Покупцю гарантійні документи на Товари разом з рахунком до сплати та видатковою накладною.

7.2. Протягом гарантійного періоду усі дефекти мають бути виправлені Постачальником без жодних витрат для Покупця не пізніше ніж через 30 днів з дати отримання повідомлення від Покупця.

8. ФОРС-МАЖОРНІ ОБСТАВИНИ

8.1 Постачальник не сплачує неустойку або не несе відповідальність за припинення Договору внаслідок невиконання зобов'язань якщо та у тій мірі у якій така затримка з виконанням або неможливістю виконання своїх зобов'язань за Договором є наслідком дії обставини непереборної сили (форс-мажору).

8.2 У цілях цієї Статті під форс-мажором розуміється будь-яка обставина або ситуація поза контролем Постачальника, що її неможливо передбачити, уникнути та вона виникає не внаслідок недбалості або браку старанності з боку Постачальника. Такі обставини можуть включати, серед іншого, дії Покупця, що перебувають виключно в його компетенції, війни або революції, пожежі, повені, епідемії, карантинні обмеження та ембарго на перевезення вантажів.

8.3 У разі виникнення ситуації Форс-мажору Постачальник негайно у письмові формі повідомляє Покупця про таку умову та її причину. Якщо Покупцем не надано іншої письмової інструкції, то Постачальник продовжує виконувати свої зобов'язання за Договором доки це практично можливо, та шукає всі доцільні альтернативні можливості виконання, яким не перешкоджає Форс-мажорна обставина.

9. ВІДПОВІДАЛЬНІСТЬ СТОРІН

9.1 За невиконання або/та неналежне виконання умов даного Договору Сторони несуть майнову відповідальність згідно з даним Договором та діючим законодавством України.

9.2. За порушення строків поставки Товарів Покупець має право розірвати договір без будь-яких зобов'язань перед Постачальником в разі невиконання поставки Товарів через 21 день від крайнього терміну поставки Товарів, вказаному в п. 2.1 цього Договору, після відповідного письмового повідомлення Покупцем.

9.3. За порушення строків поставки Товарів за пунктом 2.1 з Постачальника стягується неустойка у розмірі 0,2% від вартості Товарів, щодо яких допущено прострочення, за кожен календарний день прострочення. Неустойка, що стягується, не має перевищувати 10% вартості недопоставлених у строк Товарів.

9.4. Якщо Постачальник використовуватиме послуги субпідрядників, перевізників, експедиторів та інших компаній, які залучаються для своєчасного та належного виконання Договору, вся відповідальність перед Покупцем за будь-які втрати, збитки або за неналежне виконання Договору несе Постачальник.

10. ВИРІШЕННЯ СПОРІВ

10.1. Усі спори, що виникають внаслідок або у зв'язку з цим Договором, вирішуються шляхом переговорів між Сторонами.

10.2. Якщо Сторони не можуть дійти до згоди, то спір підлягає вирішенню у порядку, передбаченому чинним законодавством України.

11. СТРОК ДІЇ ДОГОВОРУ

11.1. Цей Договір набуває чинності в день підписання та діє до повного виконання Сторонами своїх зобов'язань, зокрема, в частині Постачання Товарів – відповідно до термінів, визначених у Статті 2, в частині розрахунків – до повного їх виконання, але не пізніше __ _____ 2023 року.

11.2. Договір складено в 2-х примірниках, які мають однакову юридичну силу, по одному для кожної Сторони.

12. ІНШІ УМОВИ

12.1 Усі зміни та доповнення до цього Договору здійснюються в письмовій формі шляхом укладення додаткових угод, що є невід'ємною частиною Договору.

12.2. Всі повідомлення будь-якої із Сторін цього Договору іншій Стороні повинні направлятись поштою, електронною поштою або факсом за адресами, вказаними у Договорі.

12.3. У випадку зміни адрес, банківських реквізитів, контактних телефонів тощо, вказаних у Договорі, Сторони зобов'язуються повідомляти про це іншу Сторону протягом 3 (трьох) робочих днів.

13. ЮРИДИЧНІ АДРЕСИ та РЕКВІЗИТИ СТОРІН

Міністерство охорони здоров'я України	Адреса: Розрахунковий рахунок
Адреса: вул. М. Грушевського, 7, м. Київ, 01601 Банківські реквізити Замовника: Код ЄДРПОУ 00012925 IBAN: UA388201720343161057100000199 в ДКСУ м. Київ	_____ _____ _____ _____

14. ПЕРЕЛІК ДОДАТКІВ

Додаток 1: Умови постачання
Додаток 2: Технічні вимоги
Додаток 3: Шахрайство та корупція

Засвідчуємо, що цей Договір підписано від імені Сторін вищевказаною датою:

Від Покупця	**Від Постачальника**
_____	_____
І.В. Кузін	
Заступник Міністра охорони здоров'я України	

Додаток 3
до договору № HEAL-RFQ-4.1.1.3/_____
від _____

ШАХРАЙСТВО ТА КОРУПЦІЯ

1. Мета

1.1 Антикорупційні настанови Банку та це доповнення застосовуються до закупівель в рамках операцій Банку з фінансування інвестиційних проектів.

2. Вимоги

2.1 Банк вимагає від Позичальників (включаючи отримувачів фінансування від Банку); учасників торгів (тих, хто подав заявки/пропозиції), консультантів, підрядників та постачальників; будь-яких субпідрядників, субконсультантів, надавачів послуг або постачальників; будь-яких агентів (заявлених чи ні); та їх співробітників дотримуватись найвищих етичних стандартів під час процесу закупівель, відбору та виконання контрактів, що фінансуються Банком, та утримуватись від шахрайства та корупції.

2.2 З цією метою Банк:

a. Визначає, для цілей цього пункту, наведені нижче терміни таким чином:

i. “корупційні дії” – це пропонування, надання, отримання або вимагання, прямо чи опосередковано, будь-чого цінного з метою неналежного впливу на дії іншої сторони;

ii. “шахрайські дії” – це будь-які дії або бездіяльність, включаючи викривлення інформації, які навмисно або ненавмисно вводять в оману або намагаються ввести в оману сторону для отримання фінансової або іншої вигоди або уникнення виконання обов’язків;

iii. “дії щодо змови” – це домовленості між двома або більше сторонами, спрямовані на досягнення неналежної мети, включаючи неналежний вплив на дії іншої сторони;

iv. “дії щодо примушування” – це негативний вплив або завдання шкоди, або погрози негативно вплинути чи завдати шкоди, прямо чи опосередковано, будь-якій стороні або її майну для здійснення неналежного впливу на дії сторони;

v. “перешкоджаючі дії” - це

(a) навмисне знищення, фальсифікація, зміна або приховування важливих для розслідування доказів або надання неправдивих заяв слідчим з метою суттєво завадити розслідуванню Банком звинувачень в корупційних або шахрайських діях, діях щодо змови або примушування, та/або погрози, домагання або залякування будь-якої сторони з метою недопущення розкриття нею відомостей, важливих для проведення розслідування, або подальшого проведення розслідування, або

(b) дії, спрямовані на суттєве перешкоджання реалізації Банком права на інспектування та аудит відповідно до пункту 2.2 e. нижче.

b. Відхиляє пропозицію щодо присудження контракту, якщо Банком буде з’ясовано, що рекомендований для укладання контракту консультант або його співробітники,

агенти, субконсультанти, субпідрядники, надавачі послуг, постачальники та/або їх співробітники прямо чи опосередковано брали участь у корупційних або шахрайських діях, діях щодо змови або примушування або перешкоджаючих діях під час участі у конкурсі щодо зазначеного контракту;

c. На додаток до засобів правового захисту, визначених у відповідній угоді про позику, може вживати відповідні заходи, включаючи оголошення про порушення процедур закупівель, якщо Банком буде встановлено, що представники Позичальника або будь-якого з отримувачів будь-якої частини коштів Позики брали участь у корупційних або шахрайських діях, діях щодо змови або примушування або перешкоджаючих діях під час процесу відбору або виконання зазначеного контракту, і що Позичальником не було вжито своєчасних та належних заходів, що є задовільними на думку Банку, з метою реагування на такі дії на момент їх виникнення, включаючи відсутність своєчасного інформування Банку про такі дії;

d. Відповідно до Антикорупційних настанов Банку та згідно з поширеною на цей час санкційною політикою та процедурами Банку, може застосувати санкції до фірми або фізичної особи на невизначений або визначений період часу, включаючи публічне оголошення про позбавлення такої фірми або фізичної особи права: (i) на присудження контракту, що фінансується Банком, або отримання від нього будь-якої фінансової чи іншої вигоди[1]; (ii) на пропонування[2] в якості субпідрядника, консультанта, виробника, постачальника або надавача послуг іншої фірми, яка має право на присудження контракту, що фінансується Банком; та (iii) на отримання коштів в рамках будь-якої позики, наданої Банком, або на будь-яку подальшу участь у підготовці або реалізації проекту, що фінансується Банком;

e. Вимагає включення до тендерної документації/запитом до надання пропозицій та до контрактів, що фінансуються за рахунок позики Банку, вимоги до учасників (тих, хто подає заявки/пропозиції), консультантів, підрядників та постачальників, їх субпідрядників, субконсультантів, надавачів послуг, постачальників, агентів дозволити Банку інспектувати[3] всі рахунки, записи та інші документи, що стосуються процесу закупівель, відбору та/або виконання контракту, а також дозволити їх аудит призначеними Банком аудиторами.

[1] Для уникнення сумнівів, позбавлення сторони, до якої застосовано санкції, права на присудження контракту має поширюватись, без обмежень, на (i) подання заявки на передкваліфікацію, висловлення інтересу в наданні консультаційних послуг та подання заявок, прямо чи в якості пропонованого субпідрядника, пропонованого консультанта, пропонованого виробника або постачальника або номінованого надавача послуг щодо цього контракту, та (ii) внесення доповнень або змін, що спричиняють суттєву модифікацію існуючого контракту.

[2] Пропонований субпідрядник, пропонований консультант, пропонований виробник або постачальних або пропонований надавач послуг (використовуються різні назви в залежності від конкретної тендерної документації) це той, хто був (i) включений консультантом до передкваліфікаційної заявки через специфічний та надзвичайно важливий досвід та ноу-хау, що забезпечують відповідність учасника кваліфікаційним вимогам за конкретною заявкою; або (ii) призначений Позичальником.

[3] У цьому контексті інспекції носять слідчий характер (експертиза). Вони включають заходи із встановлення фактів, що вживаються Банком або особами, призначеними Банком, для реагування на конкретні питання, що стосуються розслідувань/аудитів, як то оцінка правдивості звинувачень у можливому шахрайстві та корупції, шляхом використання належних механізмів. Така діяльність включає, не обмежуючись: доступ та огляд фінансової документації та інформації фірми або фізичної особи, зняття копій у разі необхідності; доступ та огляд будь-яких інших документів, даних та інформації (у паперовому або електронному вигляді), що вважаються важливими для розслідування/аудиту, та зняття копій у разі необхідності; опитування співробітників та інших відповідних осіб; здійснення фізичних інспекцій та виїздів на місце; отримання підтверджень інформації з боку третіх осіб.