ДОДАТКОВА УГОДА № 1
до договору № 7226/01 від 04.12.2023 р.

м. Запоріжжя «04» грудня 2023 р.

КОМУНАЛЬНЕ ПІДПРИЄМСТВО «ЦЕНТР УПРАВЛІННЯ ІНФОРМАЦІЙНИМИ ТЕХНОЛОГІЯМИ» іменоване надалі «Замовник», в особі директора Бєлікова Олексія Юрійовича, що діє на підставі Статуту, з однієї сторони, та **ТОВАРИСТВО З ОБМЕЖЕНОЮ ВІДПОВІДАЛЬНІСТЮ «ІТ-ІНТЕГРАТОР»**, що іменується надалі «Виконавець», в особі директора департаменту з договірної роботи Мельника Олександра Денисовича, який діє на підставі рішення єдиного учасника № 158 від 14.08.2023, з іншої сторони, в подальшому разом іменуються Сторони, а кожна окремо – Сторона, керуючись ст. 651 Цивільного кодексу України, п. 19 Особливостей здійснення публічних закупівель товарів, робіт і послуг для замовників, передбачених Законом України «Про публічні закупівлі», на період дії правового режиму воєнного стану в Україні та протягом 90 днів з дня його припинення або скасування, затверджених постановою Кабінету міністрів України від 12.10.2022 № 1178 (в редакції постанови Кабінету Міністрів України від 12.05.2023 № 471, далі – Особливості) та згідно з п. 11.3., п. 11.5. договору № 7226/01 від 04.12.2023 (далі – Договір), уклали цю додаткову угоду про наступне:

1. Відповідно до пп. 3 п. 19 Особливостей у зв'язку з покращенням якості предмета закупівлі без збільшення суми Договору, Сторони дійшли згоди:

1.1. викласти п. 1.2. Договору у новій редакції:

«1.2. Виконавець зобов'язується надати Замовнику послуги з постачання програмного забезпечення (з ліцензією на право користування антивірусним програмним забезпеченням ESET PROTECT Entry, з локальним управлінням на 12 місяців (153 об'єкта)), на яке майнові права не передаються Замовнику, код CPV за ДК 021:2015:72260000-5 – «Послуги, пов'язані з програмним забезпеченням», далі – Послуги, відповідно до Специфікації (Додаток № 1 до Договору), а Замовник – прийняти та оплатити надані Послуги в порядку та на умовах, визначених цим Договором.»

1.2. викласти Додаток № 1 до Договору в новій редакції (Додаток № 1 до Додаткової угоди).

1.3. викласти Додаток № 2 до Договору в новій редакції (Додаток № 2 до Додаткової угоди).

2. Умови Договору, не обумовлені в даній Додатковій угоді, залишаються без змін і Сторони підтверджують свої зобов'язання за ними.

3. Дана Додаткова угода набуває чинності з моменту її підписання Сторонами та скріплена печатками і є невід'ємною частиною Договору.

4. Дана Додаткова угода складена українською мовою у двох автентичних примірниках, які мають однакову юридичну силу, по одному примірнику для кожної із Сторін.

ЗАМОВНИК	**ВИКОНАВЕЦЬ**
Комунальне підприємство «Центр управління інформаційними технологіями» Адреса: 69065, м. Запоріжжя, пров. Явірний, буд. 8А IBAN UA448201720344330006000053551 ДКСУ м. Київ, МФО 820172 ЄДРПОУ 13620112 Індивідуальний податковий номер платника ПДВ 136201108299 Статус платника податку на прибуток на загальних підставах E-mail: reception@itmc.zp.gov.ua	**Товариство з обмеженою відповідальністю «ІТ-ІНТЕГРАТОР»** Код ЄДРПОУ 31091208 04080, м. Київ, вул. Костянтинівська, буд. 73; Контактний телефон/факс: (04 4) 538-00-69 IBAN UA 093510050000026002529993101 в Акціонерне товариство «УКРСИББАНК» МФО 351005; ІПН 310912026581; Свідоцтво ПДВ №200152307 Директор
Директор	
_____ О.Ю. Бєліков МП	_____ О.Д. Мельник МП

Додаток № 1 до
Додаткової угоди № 1
від «04» грудня 2023
до Договору
від «04» грудня 2023
№ 7226/01/23

Додаток № 1 до Договору
від «04» грудня 2023
№ 7226/01/23

СПЕЦИФІКАЦІЯ ПОСЛУГ

№	Найменування (склад) послуг	Од. вим.	К-сть	Ціна , грн. без ПДВ	Сума, грн., без ПДВ
1	Послуги з постачання програмного забезпечення (з ліцензією на право користування антивірусним програмним забезпеченням ESET PROTECT Entry, з локальним управлінням на 12 місяців (153 об'єкта)).	послуга	1	95369,49	95369,49
	Всього без ПДВ:				**95369,49**
	ПДВ (20%):				**19073,90**
	Всього з ПДВ				**114443,39**

Сума без ПДВ 95369,49 грн. (Дев'яносто п'ять тисяч триста шістдесят дев'ять гривень 49 копійок), крім того ПДВ: 19073,90 грн. (Дев'ятнадцять тисяч сімдесят три гривні 90 копійок), всього з ПДВ 114443,39 грн. (Сто чотирнадцять тисяч чотириста сорок три гривні 39 копійок).

ЗАМОВНИК

Комунальне підприємство «Центр управління інформаційними технологіями»
Адреса: 69065, м. Запоріжжя, пров. Явірний, буд. 8А
IBAN UA448201720344330006000053551
ДКСУ м. Київ, МФО 820172
ЄДРПОУ 13620112
Індивідуальний податковий номер платника ПДВ
136201108299
Статус платника податку на прибуток на загальних підставах
E-mail: reception@itmc.zp.gov.ua

Директор

_____ О.Ю. Бєліков

ВИКОНАВЕЦЬ

Товариство з обмеженою відповідальністю "ІТ-ІНТЕГРАТОР"
Юридична адреса: 04080, м. Київ, вул. Костянтинівська, 73
код ЄДРПОУ 31091208
р/р № UA093510050000026002529993101
в АТ «Укрсиббанк»
ІПН 310912026581
тел. (044) 538-00-69

Директор департаменту договірної роботи

_____ О.Д. Мельник

Додаток № 2 до
Додаткової угоди № 1
від «04» грудня 2023
до Договору
від «04» грудня 2023
№ 7226/ОНК

Додаток № 2 до Договору
від «04» грудня 2023
№ 7226/ОНК

ТЕХНІЧНІ ВИМОГИ
до предмета закупівлі
«Послуги, пов'язані з програмним забезпеченням»
код CPV за ДК 021:2015:72260000-5
(послуги з постачання програмного забезпечення (з ліцензією на право користування антивірусним програмним забезпеченням ESET PROTECT Entry, з локальним управлінням на 12 місяців (153 об'єкта)).

Предмет закупівлі	К-ть
Послуги з постачання програмного забезпечення (з ліцензією на право користування антивірусним програмним забезпеченням ESET PROTECT Entry, з локальним управлінням на 12 місяців (153 об'єкта)).	1 послуга

Даний додаток містить інформацію про необхідні технічні, якісні, кількісні й інші вимоги до характеристик Послуг.

Послуги надаються виконавцем для захисту 153 об'єктів.

Програмний продукт повинен відповідати наступним обов'язковим для виконання технічним вимогам:

Експертні висновки	Наявність діючих експертних висновків Державної служби спеціального зв'язку та захисту інформації України на програмні продукти антивірусного захисту, які входять до складу комплексного рішення з локальним управлінням.
Технічна підтримка	Запропонований ПП повинен мати на території України центр технічної підтримки, авторизованої виробником, та надавати технічну підтримку користувачам відповідно до наступних вимог: - обслуговування 24x7x365 - 24 години на добу, 7 днів на тиждень, 365 днів на рік, включаючи святкові, вихідні та неробочі дні, цілодобово; - розширені технічні консультації з питань конфігурації та функціонування антивірусного ПЗ по телефону (з можливості зв'язку з технічними спеціалістами по місцевому телефону без використання послуг міжнародного телефонного зв'язку) та електронній пошті; - виїзд інженера на місце розташування Замовника у випадках збоїв роботи антивірусного ПЗ.
Інтерфейс та документація до продукту	Українською або англійською мовами.

Вимоги до антивірусного програмного продукту:

1. Надання захисту від: вірусів, троянського ПЗ, рекламного ПЗ, фішингу, шпигунського ПЗ.
2. Надання захисту від шкідливого ПЗ, виявлення якого повинно здійснюватися ядром виявлення в поєднанні з компонентом машинного навчання.

3. Надання захисту від потенційно небажаних програм, яких не можна однозначно віднести до шкідливого ПЗ за аналогією з такими безумовно шкідливими програмами, як віруси або трояни, але ці програми можуть інсталювати додаткове небажане ПЗ, змінювати налаштування системи, а також виконувати неочікувані дії або дії, не підтверджені користувачем.

4. Надання захисту від потенційно небезпечних програм, а саме: несанкціонований віддалений доступ, викрадення або злам паролів, клавіатурні шпигуни тощо.

5. Надання захисту від підозрілих програм, руткітів.

6. Наявність вбудованого інструмента, що об'єднує в собі декілька утиліт для очищення залишків складних стійких загроз, таких як Conficker, Sirefef, Necurs та ін.

7. Можливість використання технології, яка забезпечує захист від загроз типу "ботнет"

8. Захист уразливостей мережевого протоколу, що покращує виявлення загроз, які використовують недоліки мережевих протоколів, таких як SMB, RPC, RDP тощо.

9. Можливість здійснювати перевірку завантажувальних секторів на наявність вірусів у головному завантажувальному записі, в тому числі у інтерфейсі UEFI.

10. Можливість для різних категорій загроз налаштовувати окремі рівні реагування як для захисту, так і для звітування.

11. Можливість робити виключення зі сканування певних файлів, які не є шкідливими, але сканування яких може спричинити відхилення в роботі або впливати на продуктивність системи.

12. Можливість створювати виключення для загальносистемних процесів з метою покращити швидкість роботи системних служб та мінімізувати втручання в процес роботи ОС.

13. Забезпечення антивірусного захисту в режимі реального часу.

14. Можливість сканування файлів під час запуску ОС.

15. Сканування комп'ютера у неактивному стані.

16. Використання евристичних технологій власної розробки під час сканування.

17. Антивірусне сканування за вимогою користувача або адміністратора та згідно графіку.

18. Модуль захисту документів, що дає можливість перевіряти макроси MS Office на наявність зловмисного коду.

19. Модуль захисту від експлойтів для забезпечення захисту від загроз здатних використовувати уразливості різноманітних додатків, таких як Java, Flash тощо.

20. Модуль, який глибоко аналізує запущені процеси та їх діяльність в файловій системі, що забезпечує додатковий рівень захисту від програм-вимагачів (Ransomware).

21. Модуль сканування оперативної пам'яті, який здатен відстежувати роботу підозрілих запущених процесів, що дозволяє запобігти зараженню навіть ретельно зашифрованими та прихованими загрозами.

22. Можливість визначення детальних параметрів роботи антивірусного сканера: визначення об'єктів та методів сканування, можливість встановлення максимального розміру та часу сканування файлу, максимальну глибину вкладення архіву та створення виключень.

23. Використання 64-бітового ядра для сканування для зменшення навантаження на систему та прискорення, підвищення ефективності сканування.

24. Можливість використання технологій машинного навчання для більш поглибленого аналізу коду з метою виявлення зловмисної поведінки та характеристик зловмисного ПЗ.

25. Наявність HIPS - системи виявлення вторгнень, яка слідкує за запуском програм та змінами в системному реєстрі, а також захищає комп'ютер від шкідливих програм і небажаної активності.

26. Можливість створювати власні правила для контролю запущених процесів, виконуваних файлів та розділів реєстру.

27. Додаткова перевірка запущених процесів у хмарному репутаційному сервісі.

28. Автоматична антивірусна перевірка змінних носіїв.

29. Наявність інструменту, який зможе здійснювати контроль підключення до робочої станції змінних носіїв шляхом створення правил доступу: блокування, дозвіл, тільки читання, читання та запис, попередження.

30. Можливість здійснювати контроль підключення до робочої станції зовнішніх пристроїв за: типом пристрою, виробником, моделлю або його серійним номером.

31. Можливість створювати групи дозволених або заборонених зовнішніх пристроїв.

32. Можливість забороняти або дозволяти підключення зовнішніх пристроїв як для всіх, так і для окремих користувачів або груп Windows або домену.

33. Можливість задавати часові інтервали, що дозволяє більш гнучко налаштовувати правила контролю пристроїв.

34. Забезпечення додаткового рівня захисту поштового трафіку на робочій станції шляхом інтеграції до поштового клієнту, з можливістю перевірки POP3, POP3S, SMTP, IMAP та IMAPS та перевірки поштових вкладень, особливо на тих ПК, що тимчасово або постійно знаходяться за межами корпоративної мережі.

35. Можливість автоматично видаляти або переміщувати заражену пошту до вказаного каталогу у поштовому клієнті.

36. Можливість використовувати білі та чорні списки спам-адресатів як користувальницькі (гнучка персоналізація інтелектуального спам-модулю), так і глобальні, інформація до яких надходить з серверів оновлення.

37. Забезпечення додаткового рівня захисту інтернет-трафіку шляхом перевірки HTTP, HTTPS трафіку, що дає можливість не тільки блокувати файли, що передаються цими протоколами, а й блокувати адреси таких небезпечних ресурсів, як фішингові сайти, сервери ботнетів, командні (C&C) сервери APT, а також сервери, що розповсюджують загрози класу «ransomware».

38. Можливість створення списків заблокованих, дозволених або виключених з перевірки URL-адрес.

39. Можливість блокувати завантаження з Інтернету файлів за вказаним розширенням, особливо на тих ПК, що тимчасово або постійно знаходяться за межами корпоративної мережі.

40. Можливість перевірки протоколу SSL як в автоматичному, так і в інтерактивному режимах. Перевірка дійсності та цілісності сертифікатів SSL-трафіку.

41. Можливість керувати списками довірених сертифікатів та сертифікатів виключених з перевірки, а також можливість вибору дії при визначенні сертифіката недіючим, невизначеним або пошкодженим .

42. Можливість створення виключень з перевірки трафіку для окремих програм та окремих IP-об'єктів (IP-адресів, діапазонів IP-адресів, підмереж).

43. Наявність персонального брандмауера для здійснення мережевої фільтрації та захисту як від зовнішніх, так і локальних мережевих атак.

44. Наявність у персональному брандмауеру інтерактивного режиму, що надає детальну інформацію про нове невідоме мережеве з'єднання та дає можливість не тільки створювати

на ПК нове правило мережевої фільтрації для виявленого з'єднання, а й вказувати детальні налаштування для нього.

45. Наявність у персональному брандмауеру режиму навчання, що дає можливість адміністратору віддалено налаштовувати дозвільні правила для мережевих додатків та обладнання.

46. Наявність редактора правил, що дає можливість не тільки редагувати створені правила, а й керувати вбудованими правилами, яких достатньо для первинного ретельного захисту від несанкціонованих мережевих з'єднань та локальних мережевих атак.

47. Можливість створювати правила мережевої фільтрації для конкретних програм і сервісів.

48. Можливість створювати для персонального брандмауеру різні профілі, які можуть автоматично переключатися, в залежності від того, до якої мережі підключено комп'ютер.

49. Можливість використовувати у персональному брандмауері додаткову автентифікацію мережі з метою запобігання несанкціонованого підключення ПК до невідомих небезпечних мереж.

50. Наявність додаткового функціоналу персонального брандмауеру, що дозволяє переглядати всю детальну інформацію по всіх наявних мережевих з'єднаннях, а також попереджати користувача про підключення до незахищеної мережі Wi-Fi.

51. Можливість налаштування додаткових параметрів модуля системи виявлення вторгнень (IDS) з метою виявлення різних типів можливих мережевих атак на комп'ютер.

52. Наявність упроваджених методів виявлення різноманітних атак, що намагаються використовувати вразливості програмного забезпечення та надання докладнішої інформації про ідентифікатори CVE.

53. Можливість переглядати на ПК автоматично заблоковані мережеві з'єднання та, за необхідністю, тимчасово дозволяти конкретні безпечні мережеві з'єднання.

54. Наявність додаткового функціоналу персонального брандмауеру, що дає можливість переглядати на ПК перелік заблокованих IP-адрес, надає інформацію про причини потрапляння до чорного списку, та дозволяє зробити виключення для конкретних безпечних адрес.

55. Наявність додаткового функціоналу персонального брандмауеру, який здатен виявляти ті зміни в мережевих програмах, що спричинили нові несанкціоновані мережеві з'єднання.

56. Фільтрація інтернет-трафіку.

57. Наявність модуля веб-контролю, що дає можливість обмежувати доступ до певних категорій сайтів.

58. Можливість створювати правила фільтрації інтернет-трафіку для різних користувачів та груп ОС Windows або домену.

59. Можливість задавати часові інтервали, що дозволяє більш гнучко налаштовувати правила веб-фільтрації.

60. Отримання оновлення клієнтів з локального сховища на сервері.

61. Можливість створення дзеркала оновлень на базі рішень для захисту кінцевих точок.

62. Можливість отримувати оновлення вірусних баз з резервних джерел, якщо основне джерело оновлення буде недосяжне.

63. Можливість для ПК отримувати оновлення з серверів виробника он-лайн, у разі перебування поза корпоративною мережею.

64. Відкат оновлень з можливістю повернутися до попередніх версій баз вірусних сигнатур і модулів оновлення, та можливістю тимчасово призупинити оновлення або встановлювати нові вручну.

65. Можливість оновлення у режимі отримання регулярних, тестових та відкладених оновлень.

66. Наявність механізму контролю за станом безпеки та актуальністю оновлень ОС.

67. Наявність інструменту для діагностики системи, який має можливість створювати знімки стану операційної системи для подальшого глибоко аналізу різноманітних аспектів роботи операційної системи, включаючи запущені процеси, контент реєстру, інстальоване ПЗ, мережеві з'єднання.

68. Можливість визначення рівня критичності значень різноманітних параметрів ОС, з метою виявлення несанкціонованих та небезпечних змін у ОС.

69. Можливість порівнювати різні знімки стану системи з метою виявлення змін, які відбулись в системі за визначений час.

70. Можливість створювати та віддалено виконувати скрипти, що дасть змогу на віддаленому ПК зупиняти запущені процеси та служби, видаляти гілки реєстру, блокувати мережеві з'єднання.

71. Локальне зберігання журналів на робочих станціях.

72. Наявність планувальника завдань, який дасть можливість створювати заплановані завдання, серед яких: запуск зовнішньої програми, перевірка файлів під час запуску системи, створення знімка стану системи, перевірка комп'ютера, оновлення вірусних баз та модулів програми.

73. Можливість планування завдань, які запускатимуться одноразово, періодично, а також за умови виникнення конкретних подій.

74. Можливість створення у планувальнику декількох однотипних завдань з різною періодичністю або різними умовами запуску.

75. Можливість створення завантажувального диску як на CD-, так і на USB-носіях з встановленим антивірусним продуктом.

76. Можливість захисту паролем параметрів рішення для захисту кінцевої точки.

77. Наявність режиму перевизначення політики, що дає системному адміністратору тимчасову можливість змінювати на ПК ті налаштування антивірусного ПЗ, що призначаються політикою, та недосяжні для редагування, з метою гнучкого налаштування антивірусного ПЗ у специфічному середовищі.

78. Графічний інтерфейс, сумісний із сенсорним екраном високої роздільної здатності.

79. Можливість гнучко налаштовувати сповіщення та повідомлення про події на робочому столі користувача.

80. Можливість віддаленого встановлення на клієнтську робочу станцію.

81. Можливість крім основного вказати резервні сервери адміністрування.

82. Наявність багатомовного інсталятора, який містить в собі в тому числі українську мову.

83. Інвентаризація обладнання, що встановлено на робочих станціях та серверах під управлінням Windows, macOS та Linux; інвентаризація ПЗ, що встановлено на робочих станціях та серверах під управлінням Windows, macOS та Linux.

84. Віддалена інсталяція антивірусного ПЗ для ОС Windows, Linux та Mac на кілька кінцевих точок одночасно; віддалена інсталяція користувальницького ПЗ;

85. Можливість віддаленого видалення встановленого користувальницького ПЗ, віддалене видалення антивірусного ПЗ для ОС Windows, Linux та Mac.

86. Можливість виконувати за допомогою інструменту віддаленого управління додаткові мережеві дії, такі як: завершення роботи та перезавантаження, відправка сигналу пробудження комп'ютера, відправка повідомлень, виконання конкретних інструкцій

командного рядка на клієнтському комп'ютері, старт оновлення операційної системи клієнтського комп'ютера.

87. Можливість використовувати двофакторну аутентифікацію для облікових записів адміністраторів, що дає можливість запобігти несанкціонованому підключенню до серверу централізованого управління.

88. Можливість налаштування автоматичного розподілу клієнтів по динамічних групах за багатьма критеріями, з наступним призначенням відповідних політик безпеки, а також запуском необхідних завдань.

89. Можливість створення дзеркала оновлень на базі сторонніх HTTP-серверів.

90. Можливість відслідковувати все встановлене на робочій станції ПЗ, а також видаляти встановлене ПЗ за вибором.

91. Можливість деактивувати ліцензію антивірусних продуктів навіть на робочих станція до яких немає фізичного або віддаленого доступу.

92. Наявність автоматичного оновлення агенту управління, що дає можливість без втручання адміністраторів використовувати актуальні версії.

93. Наявність механізму розподілу автоматичного процесу оновлення, що дозволяє знизити навантаження на мережу та комп'ютери в цілому.

94. Можливість встановлення агенту управління на ARM64 процесорах.

95. Наявність функціоналу створення площадок відповідно до філій компанії, що дозволяє назначити певну частину ліцензії окремим філіям.

96. Наявність функціоналу визначення адміністратора площадки або філії з відповідною частиною ліцензії.

97. Підтримка ОС: Microsoft Win 11, Win 10, 8.1, 8, 7(SP1+KB); Microsoft Win. Server: 2022, 2019, 2016, 2012R2, 2012, 2008(R2 SP1), Server Core (Microsoft Windows Server 2008 R2 SP1, 2012, 2012 R2); RedHat Enterprise Linux (RHEL) 7, RedHat Enterprise Linux (RHEL) 8, CentOS 7, Ubuntu Server 18.04 LTS, Ubuntu Server 20.04 LTS, Debian 10, Debian 11, SUSE Linux Enterprise Server (SLES) 12, SUSE Linux Enterprise Server (SLES) 15, Oracle Linux 8; Ubuntu Desktop 18.04 LTS 64-bit, Ubuntu Desktop 20.04 LTS, Red Hat Enterprise Linux 7 та 8, SUSE Linux Enterprise Desktop 15

ЗАМОВНИК	**ВИКОНАВЕЦЬ**
Комунальне підприємство «Центр управління інформаційними технологіями» Адреса: 69065, м. Запоріжжя, пров. Явірний, буд. 8А IBAN UA448201720344330006000053551 ДКСУ м. Київ, МФО 820172 ЄДРПОУ 13620112 Індивідуальний податковий номер платника ПДВ 136201108299 Статус платника податку на прибуток на загальних підставах E-mail: reception@itmc.zp.gov.ua	**Товариство з обмеженою відповідальністю «ІТ-ІНТЕГРАТОР»** Юридична адреса: 04080, м. Київ, вул. Костянтинівська, 73 код ЄДРПОУ 31091208 р/р № UA093510050000026002529993101 в АТ «Укрсиббанк» ІПН 310912026581 тел. (044) 538-00-69
Директор _____ О.Ю. Бєліков	Директор департаменту договірної роботи _____ О.Д. Мельник