ОБҐРУНТУВАННЯ

технічних та якісних характеристик предмета закупівлі, розміру бюджетного призначення, очікуваної вартості предмета закупівлі

(відповідно до пункту 4[1] Постанови Кабінету Міністрів України від 11 жовтня 2016 року № 710 «Про ефективне використання державних коштів» (зі змінами))

1. Найменування, місцезнаходження та ідентифікаційний код замовника в Єдиному державному реєстрі юридичних осіб, фізичних осіб - підприємців та громадських формувань, його категорія:, 07270, Київська область, Вишгородський район, м. Чорнобиль, вул. Шкільна, 6; код за ЄДРПОУ - 40248151.

2. Назва предмета закупівлі із зазначенням коду за Єдиним закупівельним словником: Створення захищеної корпоративної інформаційно-комунікаційної системи ДСП «Екоцентр» (Код за ДК 021:2015 72250000-2 Послуги, пов'язані із системами та підтримкою).

3. Ідентифікатор закупівлі: UA-2026-09-30-011553-a

4. Підстави для здійснення закупівлі:

Потреба в технічному обслуговуванні джерел безперебійного живлення, щоб забезпечити їхню подальшу стабільну роботу при виконанні лабораторних вимірювань.

Закупівля буде проводитися відповідно до Закону України «Про публічні закупівлі» (зі змінами), з урахуванням постанови Кабінету Міністрів України від 12.10.2022 № 1178 "Про затвердження 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", наказу Міністерства економіки, торгівлі та сільського господарства України № 275 від 18.02.2020 «Про затвердження примірної методики визначення очікуваної вартості предмета закупівлі».

Перелік документів, якими підтверджується наявність потреби та підстави для проведення закупівлі.

Службова записка № 08.06/288 від 06.08.2026.

5. Очікувана вартість предмета закупівлі 1 510 333,33 грн з ПДВ. (один мільйон п'ятсот десять тисяч триста тридцять три грн. 33 коп).

Розрахунок очікуваної вартості зазначеної закупівлі було складено з урахуванням рекомендацій Примірної методики визначення очікуваної вартості предмета закупівлі, затвердженої наказом Мінекономіки від 18.02.2020 № 275 (зі змінами), окремо використовуючи метод «Порівняння ринкових цін».

Враховуючи надані цінові пропозиції

ТОВ «АЙПІКОНТАКТ» (1 496 000,00 грн без ПДВ) ,

ТОВ «ІТ ЛІДЕР» (1 848 000,00 грн з ПДВ),

ТОВ «НКТ» (1 794 000,00 грн з ПДВ).

Середня вартість: **1 812 400,00 грн з П Д В .**

Визначено очікувану вартість в розмірі **1 510 333,33 грн б е з ПДВ.**

6. Процедура закупівлі:

Застосовується процедура відкритих торгів (з особливостями).

Предмет закупівлі:

Послуги зі створення захищеної корпоративної інформаційно-комунікаційної системи ДСП «Екоцентр»

(*ДК 021:2015 72250000-2 Послуги, пов'язані із системами та підтримкою*)

№ з/п	Код згідно з Єдиним закупівельним словником, що найбільше відповідає назві номенклатурної позиції предмета закупівлі	Назва номенклатурної позиції предмета закупівлі	Од. вим.	К-ть (обсяг)
1.	ДК 021:2015 72250000-2 Послуги, пов'язані із системами та підтримкою	Створення захищеної корпоративної інформаційно-комунікаційної системи ДСП «Екоцентр»	послуга	1

Обсяг робіт

- Інтеграція 120 комп’ютерів із Windows 11 Enterprise у Microsoft Entra ID.
- Налаштування другого фактора аутентифікації (MFA) для всіх 120 користувачів.
- Впровадження обмежень на використання USB-пристроїв.
- Налаштування керування оновленнями Windows через Intune та Windows Update for Business.
- Впровадження розширених політик IT-безпеки (Identity Protection, PIM, EDR, ASR).
- Оптимізація конфігурації Office 365 E3 (Exchange Online, Teams, SharePoint, OneDrive).
- Забезпечення відповідності стандартам, аудиту та резервного копіювання.
- Надання документації та проведення навчання для адміністраторів.

Терміни виконання

- Загальний термін: не більше 60 робочих днів з дати отримання заявки від Замовника засобами електронної пошти (в електронній формі).
- Етапи виконання:
    1. Аналіз поточного стану тенанта та планування: не більше 10 календарних днів.
    2. Інтеграція комп’ютерів і базова конфігурація: не більше 10 календарних днів.
    3. Налаштування безпеки, MFA, USB-обмежень, оновлень та оптимізація: не більше 10 календарних днів.
    4. Оптимізація серверного обладнання: не більше 10 календарних днів.
    5. Тестування та виправлення помилок: не більше 10 календарних днів.
    6. Передача документації та навчання: не більше 10 календарних днів.

1. Технічні вимоги до налаштування

1.1. Основні компоненти

- **Платформа**: Windows 11 Enterprise (E3 у складі Microsoft 365 E3).
- **Підписки**: Microsoft 365 E3, що включає:
    1. Microsoft Entra ID P2.
    2. Microsoft Defender for Endpoint Plan 2.
    3. Office 365 E3 (Exchange Online, Microsoft Teams, SharePoint Online, OneDrive for Business).
- **Домен**: eco-centre.com.ua (тенант діючий).
- **Кількість користувачів**: 120.
- **Пристрої**: 120 комп’ютерів із Windows 11 Enterprise, можливі мобільні пристрої (iOS, Android).

- **Середовище**: Повністю хмарне, без локальної Active Directory.

1.2. Налаштування Microsoft Entra ID P2 та керування ідентичностями

1. **Перевірка конфігурації тенанта**:

- Перевірка DNS-записів (MX, TXT, CNAME, SPF, DKIM, DMARC) для домену **eco-centre.com.ua**.
- Оптимізація адміністраторських ролей із мінімальними привілеями.

2. **Інтеграція пристроїв**:

- Підключення 120 комп'ютерів із Windows 11 Enterprise до Entra ID через Microsoft Endpoint Manager (Intune).
- Використання Azure AD Join для автоматичного приєднання всіх пристроїв.
- Налаштування Windows Autopilot для автоматизованого розгортання нових пристроїв:

  - Створення профілю Autopilot для автоматичного налаштування Windows 11.
  - Налаштування Seamless Single Sign-On (SSO) для зручного входу.

- Перевірка коректної синхронізації пристроїв із тенантом.

3. **Другий фактор аутентифікації (MFA)**:

- Увімкнення багатофакторної аутентифікації для всіх 120 користувачів:
  - Основний метод: Microsoft Authenticator (push-сповіщення або код).
  - Резервні методи: SMS або телефонний дзвінок (за потреби).
- Налаштування MFA для всіх програм Microsoft 365 і підключених SaaS-додатків.
- Політики умовного доступу (Conditional Access):
  - Обов'язкове MFA для всіх входів, включно з довіреними мережами.
  - Блокування доступу з невідомих країн або ненадійних IP.
  - Вимога відповідності пристроїв (перевірка через Defender та Intune).
- Надання інструкцій користувачам для налаштування MFA через портал "Мій обліковий запис".

4. **Розширена ідентифікація загроз (Identity Protection)**:

- Увімкнення Microsoft Entra ID Protection:
  - Виявлення ризикових входів (VPN, невідомі IP) із автоматичним блокуванням.
  - Виявлення ризикових користувачів із автоматичним скиданням пароля при витоку даних.
  - Налаштування сповіщень для адміністраторів про підозрілі дії.
- Інтеграція з Microsoft 365 Security Center для моніторингу ризиків.

5. **Privileged Identity Management (PIM)**:

- Налаштування Just-In-Time (JIT) доступу для адміністративних ролей:
  - Тимчасове підвищення прав із терміном дії (максимум 8 годин).
  - Обов'язкове схвалення підвищення прав (наприклад, через керівника).
- Увімкнення MFA для всіх адміністративних дій.
- Налаштування звітів і аудитів для відстеження дій адміністраторів.

6. **Самообслуговування**:

- Активація самообслуговування скидання паролів (SSPR) через портал "Мій обліковий запис".

7. **Зовнішні ідентичності**:

- Налаштування доступу для гостьових користувачів із обмеженими правами.
- Брендування сторінок входу та реєстрації відповідно до стилю організації.

1.3. Налаштування Microsoft Defender for Endpoint Plan 2

1. **Розгортання**:

- Активація Defender for Endpoint Plan 2 на всіх 120 комп'ютерах із Windows 11.
- Автоматичний онбординг через Intune.

2. **Захист від кіберзагроз (Next-Gen Protection)**:

- Налаштування Microsoft Defender Antivirus через Intune:
  - Увімкнення Cloud-Delivered Protection для захисту в реальному часі.
  - Автоматична відправка зразків загроз до Microsoft (лише при виявленні загроз).
  - Блокування підозрілих файлів і скриптів (наприклад, PowerShell, VBS).
- Інтеграція з умовним доступом для перевірки стану пристроїв.

3. **Endpoint Detection and Response (EDR)**:

- Увімкнення EDR для всіх 120 пристроїв:
  - Моніторинг поведінки в реальному часі.
  - Кореляція сигналів із Microsoft 365 Security Center.
- Налаштування автоматичного розслідування та усунення (AIR):
  - Автоматична ізоляція заражених пристроїв.
  - Видалення шкідливих процесів без ручного втручання.
- Налаштування сповіщень про критичні загрози для адміністраторів.

4. **Обмеження USB та периферійних пристроїв**:

- Налаштування політик у Intune:
  - Блокування всіх USB-накопичувачів, окрім сертифікованих (білий список за ID пристрою).
  - Обмеження Bluetooth-пристроїв (дозволено лише гарнітури, заборона передачі даних).
  - Блокування виконання файлів із USB-накопичувачів через Defender for Endpoint.
- Налаштування сповіщень про спроби підключення USB у Microsoft 365 Security Center.
- Ведення журналу подій для аудиту використання USB.
- Винятки для адміністраторів (за потреби) із суворим контролем через Entra ID.

5. **Зменшення поверхні атак (Attack Surface Reduction, ASR)**:

- Увімкнення правил ASR через Intune:
  - Блокування офісних макросів із Інтернету.
  - Активація Credential Guard для захисту від атак із підробкою.
  - Блокування виконання PowerShell із підозрілих джерел.
- Налаштування звітів про спрацювання правил ASR.

6. **Керування вразливостями**:

- Сканування всіх 120 комп'ютерів для виявлення вразливостей (застаріле ПЗ, конфігурації).
- Надання рекомендацій щодо патчів і оновлень через Defender.

1.4. Керування оновленнями та продуктивністю

1. **Windows Update for Business (через Intune)**:

- Створення кільцевої стратегії оновлень:
  - Тестова група (5 комп'ютерів): оновлення з затримкою 7 днів.
  - Основна група (31 комп'ютер): автоматичне встановлення після тестування.
- Налаштування графіків:
  - Щомісячні оновлення безпеки (другий вівторок місяця).
  - Оновлення функцій (один раз на рік, із тестуванням у пілотній групі).
- Встановлення відкладення: до 30 днів для безпеки, до 90 днів для функцій.
- Активні години: 8:00–18:00 (без перезавантажень у робочий час).

2. **Моніторинг і звіти**:

- Налаштування звітів про стан оновлень у Intune.
- Автоматичні сповіщення про критичні оновлення або збої.

3. **Тестування оновлень**:

- Проведення пілотного розгортання на тестовій групі перед масовим застосуванням.
- Перевірка сумісності оновлень із програмами організації.

4. **Оптимізація продуктивності через Endpoint Analytics**:

- Увімкнення Endpoint Analytics у Intune для моніторингу продуктивності:
  - Виявлення "повільних" комп'ютерів (наприклад, через низьку продуктивність CPU/диска).
  - Автоматичні рекомендації (оновлення драйверів, оптимізація конфігурації).
- Налаштування політик енергозбереження:
  - Автоматичне вимкнення комп'ютерів після 22:00 (якщо не використовуються).

1.5. Забезпечення виконання основних політик IT-безпеки

1. **Політики захисту даних**:

- Увімкнення шифрування даних у спокої (BitLocker) та під час передачі (TLS 1.2+).
- Налаштування Data Loss Prevention (DLP) у Microsoft 365 для Exchange, Teams, SharePoint, OneDrive:
  - Блокування передачі конфіденційних даних (наприклад, номери карток, паспортні дані).
  - Сповіщення адміністраторів про порушення.
  - Налаштування політик зберігання даних (Retention Policies) для відповідності GDPR та Закону України "Про захист персональних даних".

2. **Політики доступу**:

- Обов'язкове використання MFA для всіх 120 користувачів.
- Налаштування умовного доступу (Conditional Access):
  - Обмеження доступу з ненадійних мереж або пристроїв.
  - Вимога відповідності пристроїв (перевірка через Defender та Intune).
  - Обмеження доступу гостьових користувачів до мінімально необхідного.

3. **Моніторинг і аудит**:

- Налаштування Microsoft 365 Security Center для моніторингу загроз.
- Увімкнення аудиту через Microsoft Purview:
  - Журнали всіх дій адміністраторів і користувачів (вхід, доступ до файлів, USB-підключення).
  - Моніторинг спроб несанкціонованого доступу.
- Налаштування сповіщень про підозрілі дії (наприклад, незвичайні входи, USB-підключення).

4. **Відповідність стандартам**:

- Забезпечення відповідності GDPR та Закону України "Про захист персональних даних".
- Налаштування звітів про відповідність у Microsoft 365 Compliance Center.
- Впровадження базового шаблону Windows 11 Compliance Policy в Intune:
  - Вимога BitLocker для шифрування дисків.
  - Мінімальна версія ОС (наприклад, 22H2).
  - Блокування пристроїв із root-доступом або jailbreak.

1.6. Резервне копіювання та відновлення

1. **OneDrive Known Folder Move**:
   - Налаштування автоматичного збереження папок "Робочий стіл", "Документи", "Зображення" у OneDrive.
   - Політика збереження версій файлів (30 днів).
2. **SharePoint для колективних даних**:
   - Налаштування сайтів SharePoint із чіткими правами доступу (лише відповідні групи).
   - Впровадження політик резервного копіювання (щоденні бекапи, збереження 90 днів).
3. **Exchange Online**:
   - Налаштування політик резервного копіювання поштових скриньок (збереження 30 днів).

1.7. Оптимізація Office 365 E3

1. **Exchange Online**:
   - Перевірка налаштувань поштових скриньок для 120 користувачів із доменом **@eco-centre.com.ua**.
   - Оптимізація захисту від фішингу та спаму (політики Defender).
   - Оновлення DKIM, DMARC, SPF.
2. **Microsoft Teams**:
   - Оптимізація команд і каналів для комунікації.
   - Налаштування обмежень для гостьового доступу.
   - Перевірка інтеграції з Exchange і SharePoint.
3. **SharePoint Online та OneDrive**:
   - Перевірка сайтів SharePoint для командної роботи.
   - Налаштування OneDrive для кожного користувача (1 ТБ).
   - Впровадження політик шифрування та доступу.

1.8. Тестування та оптимізація

- Тестування інтеграції 120 комп’ютерів із Entra ID.
- Перевірка роботи SSO, MFA, Defender for Endpoint, Office 365, керування оновленнями, USB-обмежень.
- Симуляція атак (фішинг, зловмисне ПЗ, USB-підключення) для перевірки безпеки.
- Перевірка роботи Windows Autopilot і Endpoint Analytics.
- Оптимізація продуктивності (DNS, затримки доступу).
- Виправлення всіх виявлених помилок.

1.9. Модернізація серверної інфраструктури

- проведення технічного аудиту серверного обладнання;
- аналіз поточного використання процесорних, дискових та оперативних ресурсів;
- модернізація оперативної пам’яті серверів;
- оновлення дискових підсистем та RAID-конфігурацій;
- перевірка працездатності контролерів зберігання даних;
- оновлення мікропрограм BIOS, RAID-контролерів та систем віддаленого адміністрування;
- оптимізація серверної віртуалізації;

- створення окремих віртуальних серверів для ключових ролей інфраструктури;
- підготовка платформи для резервного копіювання та аварійного відновлення.

2. Документація та навчання

2.1. Документація

- Надання технічної документації, що включає:
  - Опис конфігурації Entra ID P2, Defender for Endpoint Plan 2, Intune, Office 365.
  - Налаштування MFA, USB-обмежень, керування оновленнями та політик IT-безпеки.
  - Опис процедур реагування на інциденти (наприклад, ізоляція пристрою, скидання пароля).
  - Список пристроїв, адміністраторських ролей і груп оновлень.
- Формат: PDF та Microsoft Word.

2.2. Навчання

Проведення 2-денного тренінгу для IT-адміністраторів (онлайн або офлайн).

Теми:

- Керування пристроями та оновленнями через Intune.
- Налаштування MFA, USB-обмежень, Identity Protection, PIM і Defender for Endpoint.
- Моніторинг і реагування на інциденти через Microsoft 365 Security Center.
- Використання Microsoft 365 Admin Center, Compliance Center і Endpoint Analytics.
- Управління резервним копіюванням у OneDrive і SharePoint.
- Надання матеріалів тренінгу (презентації, відео, інструкції).

3. Результати виконання

- Успішна інтеграція 120 комп’ютерів із Windows 11 у тенант **eco-centre.com.ua**.
- Налаштовані MFA, USB-обмеження, керування оновленнями, розширені політики безпеки (Identity Protection, PIM, EDR, ASR).
- Оптимізована продуктивність і безпека Microsoft 365 E3.
- Впроваджено резервне копіювання та аудит.
- Передана документація та навчені адміністратори.
- Система готова до експлуатації з відповідністю стандартам.

4. Критерії приймання

- Успішне підключення всіх 120 комп’ютерів до Entra ID через Azure AD Join.
- Коректна робота SSO, MFA, Defender for Endpoint, Office 365, керування оновленнями, USB-обмежень.
- Відповідність політик IT-безпеки стандартам GDPR і Закону України "Про захист персональних даних".
- Позитивні результати тестування безпеки (включаючи симуляцію атак) і продуктивності.
- Підтвердження адміністраторами замовника про готовність системи.
  Надання повної документації та матеріалів навчання.

Примітки:

Інформація про необхідні технічні, якісні та кількісні характеристики предмета закупівлі (Технічна специфікація) повинна бути надана Учасником на окремому аркуші та підписана уповноваженою особою Учасника. Учасник повинен надати опис робіт відповідно до запропонованого переліку Додатку 2 до тендерної документації, вказуючи технічні, якісні

характеристики запропонованого ним переліку робіт та іншу інформацію, що викладена у Додатку 2 до тендерної документації.

*** Документи або копії документів (які передбачені вимогами технічної специфікації), які надаються Учасником у складі тендерної пропозиції, викладені іншими мовами, ніж українська повинні надаватися разом із їх автентичним перекладом українською мовою.