Додаток 1

1. ЗАДАНІ ВИМОГИ ДО ПРЕДМЕТА ЗАКУПІВЛІ

1.1. ЗАГАЛЬНІ ВИМОГИ

1.1.1. Предмет закупівлі

Предметом закупівлі є консультаційні послуги щодо впровадження заходів захисту та керування кінцевими пристроями користувачів корпоративних хмарних сервісів Міністерства оборони України, включаючи консультації, надання рекомендацій, пропозицій щодо архітектурних рішень, їх налаштувань, надання консультацій з безпеки, допомога у впровадженні, навчання, а також здійснення обмеженої в часі технічної підтримки користувачів та які повинні:

забезпечити системне впровадження рішень з централізованого керування кінцевими пристроями користувачів корпоративних хмарних сервісів у відповідності до найкращих практик, стандартів і методологій, а також до існуючих державних і відомчих нормативно-правових актів та документів з технічного захисту інформації;

призвести до зниження ймовірності виникнення інцидентів інформаційної безпеки та витоку інформації, зокрема персональної та службової інформації, обробка якої здійснюється за допомогою кінцевих пристроїв користувачів.

сформувати у особового складу МОУ, який буде залучено до процесу впровадження і технічної підтримки впроваджених рішень, розуміння архітектури, функціональних можливостей, технічної реалізації і можливостей розвитку впроваджених рішень;

забезпечити належне документування впроваджених рішень у відповідності з найкращими практиками і стандартами;

забезпечити підготовку до проведення незалежного аудиту та державної авторизації для впроваджених рішень;

забезпечити протягом 6 місяців після впровадження первинну технічну підтримку користувачів та якісне наповнення бази знань IT інцидентів, пов’язаних з функціонуванням впроваджених рішень.

1.1.2. Вимоги щодо дотримання вимог нормативних документів

При наданні послуги необхідно враховувати положення та дотримуватися вимог таких нормативних документів:

ДСТУ 3396.2-97 Захист інформації. Технічний захист інформації. Терміни та визначення;

ДСТУ 2226-93 Автоматизовані системи. Терміни та визначення;

НД ТЗІ 1.1-003-99 Термінологія в галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу;

ДСТУ ISO/IEC 27001:2023 Інформаційні технології. Методи захисту системи управління інформаційною безпекою. Вимоги (ISO/IEC 27001:2022, IDT);

Постанова Кабінету Міністрів України № 943 від 09.10.2020 “Деякі питання об'єктів критичної інформації інфраструктури”;

Постанова Кабінету Міністрів України № 1109 від 09.10.2020 “Про затвердження Порядку віднесення об’єктів до об’єктів критичної інфраструктури”;

ДСТУ 7731:2015 “Інформаційні технологій. Методи захисту. Основні положення щодо забезпечення невтручання в особисте життя (ISO/IEC 29100:2011, MOD)”;

НД ТЗІ 3.6-005-21 “Порядок категоріювання безпеки інформаційної системи та інформації”;

НД ТЗІ 3.6-006-21 “Порядок вибору заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем”;

НД ТЗІ 3.6-007-21 “Порядок впровадження заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем”;

НД ТЗІ 2.3-025-21 “Методика оцінювання заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем”;

НД ТЗІ 2.6-004-21 “Порядок авторизації безпеки інформаційних систем”;

НД ТЗІ 3.6-008-21 “Порядок моніторингу безпеки інформаційних систем”;

FIPS PUB 199 Standards for Security Categorization of Federal Information and Information Systems. 2004;

FIPS PUB 200 Minimum Security Requirements for Federal Information and Information Systems, 2006;

NIST Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework), Version 1.1, April 2018;

NIST Special Publication 800-30. Rev.1. Guide for Conducting Risk Assessments, 2012;

NIST Special Publication 800-37. Rev.2. Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy, 2018;

NIST Special Publication 800-39. Managing Information Security Risk: Organization, Mission, and Information System View, 2011;

NIST Special Publication 800-53. Rev.5 Security and Privacy Controls for Information Systems and Organizations, 2020;

NIST Special Publication 800-64. Rev.2. Security Considerations in the System Development Life Cycle, 2008;

NIST Special Publication 800-128. Guide for Security-Focused Configuration Management of Information Systems, 2011;

NIST Special Publication 800-160 Vol. 1. Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy

Secure Systems, 2018;

NIST Special Publication 800-160 Vol. 2. Developing Cyber Resilient Systems: A Systems Security Engineering Approach, 2019.

1.1.3. Порядок надання послуги

1.1.3.1. В межах надання Послуги повинно бути надано консультування з питань системного впровадження заходів адміністрування та захисту кінцевих пристроїв користувачів корпоративних хмарних сервісів, навчання, а також первинна технічна підтримка впроваджених рішень:

Етап 1 – проведення дослідження поточного стану, аналіз ризиків, формування вимог безпеки та вимог до майбутньої архітектури та процесів;

Етап 2 – надання консультацій щодо побудови архітектури, функціональних можливостей, технічних заходів з налаштування, розгортання та адміністрування рішень із захисту кінцевих пристроїв користувачів корпоративних хмарних сервісів, впровадження, навчання;

Етап 3 – здійснення технічної підтримки користувачів корпоративних хмарних сервісів у питаннях, пов’язаних із експлуатацією впроваджених рішень.

На всіх етапах має здійснюватися документування архітектури, впроваджених рішень, їх налаштувань, проведення навчання, наповнення бази знань, пов’язаних з впровадженням рішень.

Окремі заходи різних етапів можуть виконуватись паралельно.

Всі етапи мають відбуватися в тісній взаємодії з особовим складом МОУ.

1.1.3.2. Перелік заходів та очікувані результати Етапу 1:

№ з/п	Перелік заходів	Очікуваний результат виконання (документи)
1.	Аудит наявних процесів та технічних засобів	Виконавець проводить дослідження щодо: • наявних механізмів використання в МОУ гібридної інфраструктури на базі Active Directory + Entra ID; • наявних сценаріїв використання в МОУ кінцевих пристроїв користувачів, які підключаються до хмарних сервісів МОУ із використанням хмарної служби ідентифікації та керування доступом Microsoft Entra ID або з використанням домену Active Directory; • наявних процесів захисту інформації та керування кінцевими пристроями користувачів корпоративних хмарних сервісів МОУ, із застосуванням можливостей Microsoft 365. • наявної організаційної структури

№ з/п	Перелік заходів	Очікуваний результат виконання (документи)
		підтримки вже впроваджених рішень В звітній документації описуються наявні засоби, процеси та механізми.
2.	Аналіз ризиків	З врахуванням методології керування ризиками, що впроваджена в межах наявної в Головному управлінні документації СУІБ та за результатами аналізу наявних технічних засобів, документів та процесів: • надано пропозицію щодо реєстру активів, які використовуються в межах процесу підключення кінцевих пристроїв користувачів до хмарних сервісів МОУ із використанням хмарної служби ідентифікації та керування доступом Microsoft Entra ID; • надано пропозицію щодо реєстру ризиків інформаційної безпеки, що стосуються використання кінцевих пристроїв (корпоративних / особистих), які підключаються до хмарних сервісів МОУ із використанням хмарної служби ідентифікації та керування доступом Microsoft Entra ID; • надано пропозицію щодо реєстру ризиків інформаційної безпеки, що стосуються процесів взаємодії Active Directory та Entra ID; • надано пропозицію щодо реєстру ризиків інформаційної безпеки, що стосуються процесів обробки інформації на кінцевому пристрої; • надано пропозицію щодо реєстру ризиків інформаційної безпеки, що стосуються використання штучного інтелекту (Copilot); • надано пропозицію щодо реєстру ризиків інформаційної безпеки, що стосуються процесів керування хмарною службою ідентифікації та керування доступом Microsoft Entra ID; • надано пропозиції щодо звіту з оцінки вищезазначених ризиків; • надано пропозиції щодо обробки

№ з/п	Перелік заходів	Очікуваний результат виконання (документи)
		вищезазначених ризиків (План обробки ризиків).
3.	Формування вимог безпеки	В межах прийнятих рішень **за результатами розгляду Плану обробки ризиків** надані пропозиції щодо політик (вимоги високого рівню / принципи), які стосуються: • безпечного використання кінцевих пристроїв користувачів, які підключаються до хмарних сервісів МОУ із використанням хмарної служби ідентифікації та керування доступом Microsoft Entra ID; • безпечного адміністрування хмарної служби ідентифікації та керування доступом Microsoft Entra ID; • моніторингу використання кінцевих пристроїв та здійснення адміністративної діяльності; • забезпечення антивірусного захисту кінцевих пристроїв; • керування оновленням системного та програмного забезпечення кінцевих пристроїв; • керування програмним забезпеченням (дозволеним / забороненим) кінцевих пристроїв; • керування змінами на кінцевих пристроях. Надані документальні пропозиції за напрямками захисту та керування кінцевими пристроями або сервісом Entra ID повинні містити посилання на відповідні розділи Додатку А стандарту ДСТУ ISO 27001:2023 та галузевого профілю безпеки.
4	Опис майбутньої архітектури, організації та процесів	Розроблені документи: • опис організаційної належності; • опис сценаріїв використання кінцевих пристроїв користувачів. • високорівневий опис архітектури рішення • опис рольової моделі; • опис процедур, функцій, активів, прикладних процесів;

№ з/п	Перелік заходів	Очікуваний результат виконання (документи)
		• опис обмежень; • опис оптимальної структури підтримки

1.1.3.3. Перелік заходів та очікувані результати Етапу 2:

№ з/п	Перелік заходів	Очікуваний результат виконання (документи)
5	Технічні заходи розгортання та налаштування рішень із захисту та керування кінцевих пристроїв користувачів корпоративних хмарних сервісів з використанням Microsoft Intune та політик умовного доступу	Настанови, дорадчі записи, технічний опис рішень та консультування з наступних завдань: 1. Управління мобільними пристроями через Intune - налаштування ролей для адміністраторів - делегування та розмежування повноважень - реєстрація пристроїв з різними ОС - політики конфігурації пристроїв - перевірка відповідності пристроїв вимогам та політики безпеки - віддалене блокування та очищення пристроїв 2. Управління мобільними додатками через Intune - встановлення і оновлення додатків - захист додатків, налаштування політик безпеки для додатків - розмежування корпоративних і особистих даних на особистих пристроях користувачів - управління корпоративними даними 3. Політики умовного доступу - обмеження доступу до корпоративних ресурсів за різними критеріями - вимоги реавтентифікації - управління доступом користувачів з урахуванням risk based access control 4. Захист даних і безпека - шифрування даних на пристроях користувачів - блокування доступу до пристроїв - антивірусний захист - створення і розповсюдження шаблонів безпеки 5. Управління оновленнями і патчами 6. Звіти і моніторинг, дешборди в PowerBI 7. Інтеграція з SCCM, co-management 8. Автоматичне налаштування і конфігурація Windows-пристроїв без необхідності втручання користувача (Autopilot) 9. Security Copilot в Intune
6	Типові завдання із загального адміністрування кінцевих пристроїв користувачів корпоративних	Настанови, дорадчі записи та консультування з наступних завдань: 1. Розгортання агентів управління 2. Синхронізація пристроїв в Intune

№ з/п	Перелік заходів	Очікуваний результат виконання (документи)
	хмарних сервісів з використанням Microsoft Intune	3. Делегування привілейованих ролей 4. Налаштування профілів користувачів та пристроїв 5. Розгортання програмних застосунків 6. Налаштування та моніторинг безпеки пристроїв та облікових записів користувачів 7. Управління доступом до хмарних служб 8. Вивід пристроїв з експлуатації та блокування їх роботи 9. Розроблення та застосування сценаріїв автоматизації для Intune з використанням PowerShell 10. Розроблення та застосування шаблонів управління для Intune на базі Terraform, Bicep 11. Управління оновленнями пристроїв (в т.ч. операційних систем) 12. Вирішення інших типових проблем

1.1.3.4. **Перелік заходів та очікувані результати Етапу** 3:

№ з/п	Перелік заходів	Очікуваний результат виконання
1.	Надання технічної підтримки користувачам в частині вирішення питань, пов’язаних із впровадженням рішень безпеки	Звіт за результатами роботи, кількісні і якісні характеристики
2.	Створення і наповнення бази знань	База знань в електронній формі з описом типових звернень користувачів та варіантів їх вирішень

1.1.4. Вимоги до процедури звітування та оцінки відповідності наданих послуг

Виконавець інформує Замовника про виконання заходів передбачених п.п. 3.1.3.2–3.1.3.4 та готовність до передачі напрацювань (документів).

Для кожного реалізованого заходу відповідно до переліку заходів та очікуваних результатів, Виконавцем надається звіт до якого додаються відповідні документи створені в межах надання Послуги та передбачені етапом або посилання на відповідні документи, надані раніше в межах виконання етапу.

Підсумковий звіт із зазначенням результатів виконання заходів за етапом та акт виконаних робіт за результатами виконання відповідного етапу надається Виконавцем в термін зазначений в календарному плані надання послуг за договором.

Для оцінки відповідності наданих послуг за цією ТС Замовником може бути організована комісія з приймання результатів відповідних заходів або етапів.

1.2. ВИМОГИ ДО НАДАННЯ ПОСЛУГИ

Виконавець самостійно визначає та забезпечує інструменти, необхідні для надання Послуги.

Виконавець виконує всі дії у тісній взаємодії з фахівцями Головного управління.

Заборонено використання неліцензійного, піратського програмного забезпечення, а також програмного забезпечення, правовласником якого є організації, пов’язані з російською федерацією.

Для забезпечення надання Послуги Виконавцеві надається обмежений та контрольований доступ до хмарної служби ідентифікації та керування доступом Microsoft Entra ID та адміністративної панелі управління кінцевими пристроями користувачів корпоративних хмарних сервісів Intune у відповідності до внутрішніх правил та процедур МОУ.

1.3. ВИМОГИ ДО РОЗГОРТАННЯ

Всі дії Виконавця мають бути погоджені із Головним управлінням та не повинні призводити до збоїв у робочих середовищах.

Всі рішення і налаштування мають спочатку бути впроваджені та відтестовані на невеликій пілотній групі користувачів (пристроїв), наступним етапом на групі з більшою кількістю користувачів (пристроїв), і лише на третьому етапі, в разі відсутності великої кількості збоїв, рішення може бути застосоване на ту групу користувачів чи пристроїв, для якої проєктувалося.

Введення в експлуатацію всіх аспектів рішень з централізованого керування кінцевими пристроями користувачів корпоративних хмарних сервісів та відповідні зміни в налаштуваннях систем повинні бути погоджені відповідальними посадовими особами Головного управління.

1.4. ВИМОГИ ЩОДО ЗАБЕЗПЕЧЕННЯ ДЕРЖАВНОЇ ТАЄМНИЦІ ТА КОНФІДЕНЦІЙНОСТІ

Вимоги щодо забезпечення охорони державної таємниці під час надання Послуги не висуваються.

Виконавець повинний забезпечити конфіденційність інформації, яка була отримана під час надання Послуги.

У випадку залучення Виконавцем до надання Послуги третьої сторони Виконавець зобов'язаний забезпечити дотримання третьою стороною всіх вимог щодо забезпечення конфіденційності наданої інформації.

1.5. ТЕРМІН НАДАННЯ ПОСЛУГИ

Термін надання послуги не повинен перевищувати 12 (дванадцяти) місяців з дати підписання договору включно з терміном надання первинної технічної підтримки – не менше 6 (шести) місяців.

1.6. АДРЕСА НАДАННЯ ПОСЛУГИ

Адреса надання послуг: м. Київ, проспект Повітряних Сил, 6 (конкретна адреса буде надана під час організації надання послуг)*.

Виходячи з міркувань безпеки та відповідно до Постанови Кабінету Міністрів України від 04.03.2015 № 83 "Про затвердження переліку об'єктів державної власності, що мають стратегічне значення для економіки і безпеки держави Замовник є підприємством, що має стратегічне значення для економіки і безпеки держави", пункту 27 Особливостей здійснення публічних закупівель, затверджених Постановою Кабінету Міністрів України від 12.10.2022 № 1178 (У разі коли оприлюднення в електронній системі закупівель інформації про місце поставки, оприлюднення якої передбачено Законом, несе загрозу безпеці замовника, така інформація може зазначатися як найменування населеного пункту, в який здійснюється доставка товару (в якому виконуються роботи чи надаються послуги), а вся необхідна інформація для виконання договору надається Переможцю відповідної процедури після підписання договору щодо нерозголошення конфіденційної інформації).