ПРОЄКТ

**ДОГОВІР № \_\_\_\_\_\_**

|  |  |
| --- | --- |
| м. Кривий Ріг | «\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 2024 p. |
|  |  |

Виконавчий комітет Криворізької міської ради (надалі – Замовник), в особі \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, яка діє на підставі Закону України «Про місцеве самоврядування в Україні» та Положення про виконавчий комітет Криворізької міської ради, з однієї сторони, і \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_(надалі – Виконавець), в особі\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, яка (який) діє на підставі \_\_\_\_\_\_\_\_\_\_\_\_, з іншої сторони, (надалі разом іменуються – Сторони, а кожна окремо – Сторона), уклали цей договір (надалі – Договір) про наступне:

**1.** **ПРЕДМЕТ ДОГОВОРУ**

1.1. Замовник доручає, а Виконавець бере на себе зобов'язання власними силами, матеріалами та засобами надати послугу ДК 021:2015:72220000-3, Консультаційні послуги з питань систем та з технічних питань  (консультаційні послуги щодо створення системи управління інформаційною безпекою та конфіденційністю у відповідності до вимог ДСТУ ISO/IEC 27001:2023, ДСТУ ISO/IEC 27701:2022 та сертифікації телекомунікаційного обладнання) (далі – Послуга).

1.2. Вимоги до Послуги, що є предметом Договору, визначаються Технічним завданням (Додаток 1), що є невід’ємною частиною Договору.

1.3. Зміни та доповнення до Договору, його додатків, мають бути оформлені додатковими угодами, що є невід’ємними частинами Договору.

1.4. Результати надання Послуги визначаються Технічним завданням (Додаток 1), що є невід’ємною частиною Договору.

1.5. Обсяг закупівлі Послуги може бути зменшено залежно від реального фінансування видатків Замовника.

1.6. Кількість послуг-1 послуга.

**2.** **ЯКІСТЬ ПОСЛУГИ**

2.1. Виконавець повинен надати Замовнику Послугу, якість якої повинна відповідати умовам Технічного завдання, стандартам та технічній документації, що застосовується до даного виду послуг згідно з чинним законодавством (у тому числі ДСТУ ISO/IEC 27001:2023 (ISO/IEC 27001:2022, IDT) «Інформаційна безпека, кібербезпека та захист конфіденційності. Системи керування інформаційною безпекою. Вимоги», ДСТУ EN ISO/IEC 27701:2022 (EN ISO/IEC 27701:2021, IDT; ISO/IEC 27701:2019, IDT) «Методи безпеки. Розширення до ISO/IEC 27001 та ISO/IEC 27002 для управління конфіденційною інформацією. Вимоги та вказівки», Технічного регламенту з електромагнітної сумісності обладнання, затвердженого постановою Кабінету Міністрів України від 16.12.2015 №1077 (Наказ Мінекономрозвитку України від 19.06.2018 №848), Технічного регламенту радіообладнання, затвердженого постановою Кабінету Міністрів України від 24.05.2017 №355 (Наказ Мінекономрозвитку України від 03.07.2018 №908), інших нормативно-правових та технічних документів, які встановлюють вимоги до створення та впровадження системи управління інформаційною безпекою).

2.2. Перелік наукової, технічної та іншої продукції (документації), яка підлягає оформленню i здачі Виконавцем Замовнику на окремих етапах та/або по закінченню надання Послуги за цим Договором, визначається у Технічному завданні.

**3.** **ЦІНА ДОГОВОРУ**

3.1. Загальна ціна цього Договору становить \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ грн. (цифрами і прописом) з урахуванням ПДВ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ грн. (цифрами і прописом)/ без ПДВ.

3.2. Загальна ціна Договору може бути зменшена за взаємною згодою Сторін.

3.3. Калькуляцію кошторисної вартості Послуги наведено в Додатку 2, що становить невід’ємну частину цього Договору.

3.4. Загальний обсяг фінансування Послуги не може перевищувати загальної вартості, наведеної в п. 3.1. Договору.

**4.** **ПОРЯДОК ЗДІЙСНЕННЯ ОПЛАТИ**

4.1. Розрахунок за надану Послугу проводяться Замовником після підписання Сторонами акта приймання-передачі наданої послуги (далі – Акт). До Акта Виконавцем додається належним чином оформлений рахунок на оплату Послуги.

4.2. Оплата згідно з Актом здійснюється протягом 20 (двадцяти) банківських днів з моменту підписання Акту обома Сторонами.

4.3. У разі затримки бюджетного фінансування, не з вини Замовника, оплата за надану Послугу здійснюється протягом 3 (трьох) банківських днів з дати отримання Замовником бюджетного фінансування на свій реєстраційний рахунок.

**5. СТРОКИ ТА УМОВИ НАДАННЯ ПОСЛУГИ**

5.1. Вимоги до результатів надання Послуги визначено в Технічному завданні.

5.2. Строк надання Послуги: протягом 125 робочих днів з дати підписання Договору, але не пізніше ніж до 31 грудня 2024 року.

5.3. Документація за результатами надання Послуг, передбачена Технічним завданням, передається Замовнику Виконавцем по готовності у електронному або паперовому вигляді з дотриманням вимог щодо збереження конфіденційності інформації. Сторонами узгоджено, що пересилання результатів наданих Послуг у електронному вигляді можливе за допомогою довіреного каналу зв’язку на електронну адресу \_\_\_\_\_\_\_\_\_\_. Сторони зобов’язуються слідкувати за надходженням електронних документів та своєчасно здійснювати їх приймання та перевірку.

5.4. Замовник протягом 15 (п’ятнадцяти) календарних днів від дня одержання Акта приймання-передачі направляє Виконавцю підписаний Акт або мотивовану відмову від приймання Послуги. Послуга вважається наданою та підлягає сплаті, у разі відсутності зауважень від Замовника щодо отриманих результатів наданої Послуги та підписання Сторонами Акта приймання-передачі.

5.5. Місце надання Послуги: 50101 Дніпропетровська обл. м. Кривий Ріг, пл. Молодіжна,

буд. 1.

**6.** **ПРАВА ТА ОБОВ’ЯЗКИ СТОРІН**

6.1. Замовник має право:

6.1.1. Достроково розірвати Договір у разі невиконання зобов'язань Виконавцем, повідомивши про це його у строк, визначений пунктом 11.4.3 цього Договору.

6.1.2. Контролювати надання Послуги (знайомитись з виконавчими журналами та іншими технічними документами Виконавця).

6.1.3. Зменшувати обсяг закупівлі та/або ціну Договору з урахуванням фактичного обсягу видатків, а також виробничої необхідності. У такому разі Сторони вносять відповідні зміни до цього Договору шляхом укладання додаткової угоди.

6.1.4. Повернути протягом терміну, передбаченого пунктом 5.4 цього Договору, Акт Виконавцю без здійснення оплати у разі неякісного надання Послуги або неналежного оформлення документів, зазначених у Технічному завданні.

6.1.5. У разі дострокового надання Послуги достроково прийняти та оплатити їх у межах вартості, передбаченої Договором, та затвердженого обсягу фінансування на поточний рік.

6.2. Замовник зобов'язаний:

6.2.1. Своєчасно та в повному обсязі оплачувати надану Послугу, якщо це не суперечить пунктам розділу 4 та пунктам 6.1.3, 6.1.4 цього Договору.

6.2.2. Приймати надану Послугу згідно з Актом, обсяг та якість якої відповідає вимогам цього Договору.

6.2.3. Надавати Виконавцю інформацію, в межах своєї компетенції, необхідну для виконання ним договірних зобов'язань.

6.3. Виконавець зобов'язаний:

6.3.1. Забезпечити надання Послуги у строки встановлений цим Договором.

6.3.2. Забезпечити надання Послуги, якість якої повинна відповідати розділу 2 цього Договору.

6.3.3. Своїми силами та за власний рахунок усувати недоліки та прорахунки, які виникли з вини Виконавця.

6.3.4. У разі виникнення обставин, що перешкоджають належному виконанню Виконавцем своїх зобов’язань за цим Договором, повідомити про це Замовника.

6.3.5. Надати Послугу відповідно до вимог Технічного завдання.

6.3.6. Не поступатися третім особам правом вимоги до Замовника, що виникають з цього Договору.

6.4 Виконавець має право:

6.4.1. Своєчасно та в повному обсязі отримувати плату за надану Послугу, якщо це не суперечить пунктам розділу 4 та пунктам 6.1.3, 6.1.4 цього Договору.

6.4.2. На дострокове надання Послуги за письмовим погодженням Замовника.

6.4.3 У разі невиконання зобов’язань Замовником Виконавець має право достроково розірвати цей Договір, повідомивши про це Замовника у строк не пізніше ніж за 7 (сім) робочих днів до дати розірвання договору, якщо це не суперечить пунктам розділу 4, пунктам 6.1.3, 6.1.4 та розділу 8 цього Договору.

6.4.4. За письмовим погодженням із Замовником залучати або змінювати співвиконавців, окремих фахівців для належного виконання умов Договору.

**7.** **ВІДПОВІДАЛЬНІСТЬ СТОРІН**

7.1. У разі невиконання чи неналежного виконання своїх зобов'язань за Договором Сторони несуть відповідальність згідно з чинним законодавством України та цим Договором.

7.2. Види порушень та санкції за них, установлені Договором:

7.2.1. При порушенні якісних критеріїв надання Послуги, зазначених у цьому Договорі, Технічному завданні, Виконавець на вимогу Замовника зобов’язується сплатити на його користь штраф у розмірі 20 % вартості Послуги.

7.2.2. При порушенні строків надання Послуги, Виконавець на вимогу Замовника зобов’язується сплатити на його користь пеню у розмірі 0,1 % вартості Послуги , але не більше 2-х облікових ставок НБУ, що діяла у період, за який сплачується штраф від вартості неналежно виконаних зобов’язань, з яких допущено прострочення виконання за кожний день прострочення.

7.3. Замовник звільняється від відповідальності за порушення передбачених цим Договором строків здійснення розрахунків, якщо такі порушення викликані відсутністю (затримкою) бюджетного фінансування.

7.4. Усі та будь-які претензії третіх осіб з приводу порушення їх майнових та особистих немайнових прав, що виникли при виконанні цього Договору, в тому числі такі, що будуть пред`явлені Замовнику, будуть врегульовані Виконавцем від власного імені і за власний рахунок.

**8.** **ОБСТАВИНИ НЕПЕРЕБОРНОЇ СИЛИ**

8.1. Сторони звільняються від відповідальності за невиконання або неналежне виконання зобов'язань за цим Договором у разі виникнення обставин непереборної сили, які не існували під час укладання Договору та виникли поза волею Сторін (аварії, катастрофи, стихійні лиха, епідемії, війна або військові дії, блокади, страйки, громадські заворушення тощо).

8.2. Сторона, що не може виконувати зобов'язання за цим Договором унаслідок дії обставин непереборної сили, повинна не пізніше ніж протягом 3 (трьох) робочих днів з моменту їх виникнення повідомити про це іншу Сторону у письмовій формі.

8.3. Доказом виникнення обставин непереборної сили та строку їх дії є відповідні документи, які видаються Торгово-промисловою палатою України або її територіальними органами.

8.4. У разі коли строк дії обставин непереборної сили продовжується більше ніж 30 (тридцять) календарних днів, кожна із Сторін в установленому порядку має право розірвати цей Договір або подовжити строк його виконання.

8.5. Сторона не має права посилатися на обставини непереборної сили у випадку, коли вони виникли у момент прострочення нею виконання її обов’язків за цим Договором.

**9.** **ВИРІШЕННЯ СПОРІВ**

9.1. У випадку виникнення спорів або розбіжностей Сторони зобов'язуються вирішувати їх шляхом взаємних переговорів та консультацій.

9.2. У разі недосягнення Сторонами згоди спори (розбіжності) вирішуються у судовому порядку.

**10.** **СТРОК ДІЇ ДОГОВОРУ**

10.1. Цей Договір набирає чинності з дати підписання Договору уповноваженими представниками Сторін і діє до 31 грудня 2024 року, в частині виконання зобов’язань – до повного їх виконання.

**11**. **ІНШІ УМОВИ**

11.1. Цей Договір укладається та підписується у 2 (двох) автентичних примірниках по одному для кожної із Сторін, які мають однакову юридичну силу.

11.2. Умови Договору можуть бути змінені за згодою Сторін шляхом укладення в письмовій формі додаткових угод, підписаних уповноваженими представниками обох Сторін і скріплених їхніми печатками. Одностороння зміна Договору не допускається. Істотні умови договору можуть змінюватись лише у випадках передбачених 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 жовтня 2022 року №1178 (зі змінами). Всі зміни та доповнення до цього Договору оформляються шляхом укладання додаткових угод, які є його невід’ємною частиною.

11.3. Виходячи із сутності обставин Замовник самостійно визначає форму підтвердження об’єктивних обставин (документ від постачальника з детальним поясненням виникнення таких причин), що спричиняють зміну істотних умов Договору в частині подовження строків надання Послуги, при цьому такі зміни не призведуть до збільшення суми визначеної в Договорі.

11.4. Порядок розірвання Договору.

11.4.1. Цей Договір може бути розірваний за домовленістю Сторін або за рішенням суду.

11.4.2. Цей Договір може бути розірваний односторонньо за ініціативою Замовника у разі:

– затримки надання Послуги чи їх окремих етапів на строк більше 30 (тридцяти) днів, якщо у межах цього часу не досягнуто домовленості між Замовником і Виконавцем про продовження термінів виконання;

– невідповідності наданої Послуги вимогам Технічного завдання.

11.4.3. При односторонньому розірванні Договору Замовник повинен письмово повідомити Виконавця про своє рішення у строк не пізніше, ніж за 7 (сім) робочих днів до дати розірвання Договору. Датою розірвання Договору є дата, зазначена у письмовому повідомленні.

11.5. Виконавець гарантує та підтверджує дотримання усіх прав третіх осіб (за наявності таких прав) при виконані Виконавцем своїх зобов’язань за цим Договором.

**12.** **ДОДАТКИ ДО ДОГОВОРУ**

Невід’ємною частиною цього Договору є:

Додаток 1 – Технічне завдання.

Додаток 2 – Калькуляція кошторисної вартості Послуги.

**13. МІСЦНЗНАХОДЖЕННЯ ТА БАНКІВСЬКІ РЕКВІЗИТИ СТОРІН**

**ЗАМОВНИК: ВИКОНАВЕЦЬ:**

**Виконавчий комітет Криворізької**

**міської ради**

Адреса: 50101 Дніпропетровська обл.

м. Кривий Ріг пл. Молодіжна, 1

р/р UA

Держказначейська служба України

м. Київ

МФО 820172

Код ЄДРПОУ 04052169

Телефон: (0564) 93 04 69

E-mail: mvk99@kr.gov.ua

\_\_\_\_\_\_\_\_\_\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Додаток 1

до Договору від \_\_\_\_\_\_ № \_\_\_

**ТЕХНІЧНЕ ЗАВДАННЯ**

ДК 021:2015:72220000-3, Консультаційні послуги з питань систем та з технічних питань  (консультаційні послуги щодо створення системи управління інформаційною безпекою та конфіденційністю у відповідності до вимог ДСТУ ISO/IEC 27001:2023, ДСТУ ISO/IEC 27701:2022 та сертифікації телекомунікаційного обладнання)

*Склад послуги:*

 **Створення системи управління інформаційною безпекою та конфіденційністю** (далі – СУІБ) включає: розробки процесів інформаційної безпеки, проектних документів у межах сфери застосування СУІБ, до якої належать підрозділи Виконавчого комітету Криворізької міської ради, працівники яких задіяні у процесах функціонування «Підсистеми документообігу», «Підсистема кадрового забезпечення» та Web Порталу, відповідно до вимог ДСТУ ISO/IEC 27001:2023, ДСТУ ISO/IEC 27701:2022, а саме:

* Аналіз організаційної та інформаційної інфраструктури, здійснених заходів щодо розподілу об’єкта СУІБ на фізичному та/або логічному рівні (сегментація мережі, визначення інформаційних потоків та встановлення периметру фізичної безпеки). Формування загального уявлення про наявність потенційних загроз.
* Документування сфери застосування СУІБ (аналіз реєстру інформаційних активів Замовника, інвентаризаційних відомостей із визначеними Власниками активів, класифікації інформації), виходячи із встановлених об'єктів захисту відповідно до вимог ДСТУ ISO/IEC 27001:2023 на основі аналізу:

– зовнішніх та внутрішніх обставин;

– потреб та очікувань заінтересованих сторін;

– інтерфейсів та залежностей між діями організації та інших організацій для виконання цілей бізнес-процесів.

* Створення плану побудови СУІБ та формування концептуальних рішень щодо побудови СУІБ.
* Проведення заходів з оцінки та обробки ризиків, формування реєстру ризиків відповідно до вимог ДСТУ ISO/IEC 27005:2023:

– створення та документування структури управління ризиками (методологія) для забезпечення узгодженості;

– опис прикладів сценаріїв, за яких інформація, системи або служби можуть бути скомпрометовані;

– визначення ймовірності, з якою можуть відбуватися ці сценарії;

– оцінка потенційного впливу кожного сценарію на конфіденційність, цілісність або доступність інформації, систем і послуг;

– ранжирування сценаріїв ризику на основі загального ризику для цілей організації

* Документування плану обробки ризиків відповідно до вимог ДСТУ ISO/IEC 27005:2023:

– розробка заходів захисту на кожен ризик (обробка ризику) із призначенням відповідального Власника (у межах ролевої моделі СУІБ) для кожного виявленого ризику;

– призначення відповідального за здійснення діяльності щодо зменшення ризиків;

– встановлення цільових термінів завершення заходів з усунення ризиків.

* Консалтинг зі створення Положення щодо організації заходів кібербезпеки, поточного профілю кібербезпеки, цільового профілю, з урахуванням вимог ДСТУ ISO/IEC 27001:2023 та ISO/IEC 27002:2022, наказу Адміністрації державної служби спеціального зв’язку та захисту інформації України від 06 жовтня 2021 року № 601 "Про затвердження Методичних рекомендацій щодо підвищення рівня кіберзахисту критичної інформаційної структури" (зі змінами внесеними наказом від 10.07.2022 № 343) та рекомендацій NIST Special Publication 800-53 Revision 5 “Security and Privacy Controlsfor Information Systems and Organizations”.
* Створення Положення щодо застосовності:

– перегляд засобів контролю Додатку А ДСТУ ISO/IEC 27001:2023;

– обрання засобів контролю для усунення виявлених ризиків;

– визначення засобів контролю Додатку А ДСТУ ISO/IEC 27001:2023 та надання послуг щодо проведення заходів з обґрунтування включення або виключення кожного елемента керування при реалізації СУІБ та поточний стан реалізації.

* Створення політик верхнього рівня та внутрішньої документації СУІБ (перегляд вмісту існуючої документації Замовника, положень, інструкцій та їх коригування відповідно до вимог ДСТУ ISO/IEC 27001:2023). Розробка відповідно до вимог ISO/IEC 27001:2022:

– порядку модернізації та оновлення програмних та апаратних компонентів інформаційно-комунікаційної системи (ІКС) під час їх експлуатації;

– процедур управління документацією, записами, управління персоналом;

– процедур управління доступом;

– політики управління ризиками інформаційної безпеки, порядку звітування;

– процедур реєстрації і аналізу інцидентів;

– процедур резервного копіювання;

– процедур управління з’ємними носіями інформації;

– процедур внесення відомостей до журналу реєстрації резервного копіювання, журналу реєстрації технічного контролю після змін в операційній системі, журналу реєстрації інцидентів, журналу реєстрації тестів по безперервності бізнесу, журналу технічного обслуговування тощо.

– правил щодо допустимого використання інформації та активів;

– ролі, обов'язки та повноваження;

– процедур контролю задокументованої інформації;

– процедур контролю з боку керівництва;

– процедур проведення внутрішнього аудиту та процедур щодо звітування про внутрішні аудити;

– дії персоналу, які мають певну роль в СУІБ щодо постійного вдосконалення СУІБ;

– процедур відповідальності за порушення політик СУІБ;

– процедур з контролю за якістю аутсорсингових послуг, кваліфікацією співробітників постачальника послуг та діями стосовно зменшення ризику пов’язаного з плинністю кадрів, а також опис процесів навчання та покращення навичок та знань.

* Створення програм навчань та підвищення обізнаності співробітників:

– регулярні тренінги для ознайомлення з новими політиками та процедурами захисту від шкідливих програм та протидії соціальній інженерії;

– визначення очікувань для персоналу щодо його ролі в обслуговуванні СУІБ;

– навчання персоналу загальним загрозам, з якими стикається організація, і способам реагування;

– ознайомлення з політикою або процедурою дисциплінарної відповідальності або санкцій для персоналу, якого викрили;

– дотримання вимог інформаційної безпеки.

*Результатом є:* комплект проектних документів СУІБ відповідно до вимог ДСТУ ISO/IEC 27001:2022, ДСТУ EN ISO/IEC 27701:2022, згідно переліку наведеного у Таблиці.

|  |  |
| --- | --- |
| **№ з/п** | **Назва документа** |
|  | **Управління документами** |
| 1 | Основний перелік термінів, визначень та скорочень |
| 2 | Порядок оформлення документів та контроль записів |
|  | **Підготовка до проекту** |
| 3 | Наказ (проект) “ Організація захисту інформаційної безпеки та кіберзахисту” |
| 4 | План побудови СУІБ (із наведенням основного переліку документів СУІБвідповідно до вимог ДСТУ ISO 27001:2023) |
| 5 | Концептуальні рішення щодо побудови СУІБ |
|  | **Ідентифікація вимог** |
| 6 | Процедури для ідентифікації вимог |
| 7 | Додаток – Перелік правових, нормативних, договірних таінших вимог |
| 8 | Політика управління активами |
|  | **СУІБ Scope** |
| 9 | Сфера застосування СУІБ  |
|  | **Основні політики** |
| 10 |  Політика інформаційної безпеки  |
| 11 | Політика захисту персональних даних |
| 12 | Політика захисту персональних даних працівників |
| 13 | Політика збереження даних |
| 14 | Норми поведінки |
|  | **Повідомлення про конфіденційність** |
| 15 | Повідомлення про конфіденційність |
| 16 | Повідомлення про конфіденційність співробітників |
| 17 | Повідомлення про конфіденційність співробітників постачальника |
|  | **Уповноважена особа із захисту**  **персональних даних** |
| 18 | Уповноважена особа із захисту персональних даних  |
| 19 | Лист про призначення уповноваженої особи із захисту персональних даних (зразок) |
| 20 | Умови призначення уповноваженої особи із захисту персональних даних |
|  | **Заходи з визначення активів СУІБ**   |
| 21 | Положення щодо інвентаризації та обробки даних |
| 22 | Інвентаризаційні відомості (зразок) |
| 23 | Апаратне забезпечення та мережева інфраструктура (топологія мережі) |
|  | **Оцінка та обробка ризиків** |
| 24 | Методологія оцінки та обробки ризиків  |
| 25 | Таблиця оцінки ризиків та обробки ризиків (зразок) |
| 26 | План про оцінку та обробку ризиків (зразок) |
| 27 | Звіт про оцінку та обробку ризику (зразок) |
|  | **Оцінка впливу на захист**  **персональних даних** |
| 28 | Методологія оцінки впливу на захист персональних даних |
| 29 | Реєстр оцінки впливу на захист персональних даних (зразок) |
|  | **Застосовність засобів контролю** |
| 30 | Положення про застосовність (SoA) |
|  | **План реалізації** |
| 31 | Положення щодо організації заходів кібербезпеки із наведенням профілю кібербезпеки (відповідно до вимог ДСТУ ISO/IEC 27001:2023, ДСТУ ISO/IEC 27005:2023 та рекомендацій наказу Адміністрації Держспецзв’язку України від 06 жовтня 2021 року № 601).Інструкції: відповідальному за інформаційну безпеку, відповідальному за захист персональних даних, відповідальному за актив, користувачу, адміністратору, Інструкція з антивірусного захисту |
|  | **Політики та процедури безпеки** |
| 32 | Політика ІТ безпеки(A.5.10 Політика прийнятного використанняA.8.7 Політика захисту від шкідливих програм) |
| 33 | Політика чистого стола та чистого екрану |
| 34 | Політика щодо мобільних пристроїв, дистанційної роботи та роботи з дому(включаючи A.6.7 Політика віддаленого доступу) |
| 35 | Політика використання власного пристрою |
| 36 | Процедури роботи в безпечних зонах (A.7.4 Моніторинг фізичної безпеки)  |
| 37 | Політика класифікації інформації |
| 38 | Процедури безпеки для відділу ІТ  |
| 39 | Політика управління змінами |
| 40 | Політика резервного копіювання |
| 41 | Політика утилізації та знищення (Примітка: це може бути реалізовано як частину процедур безпеки для ІТ відділу)  |
| 42 | Політика криптографії(Політика використання засобів криптографічного захисту; Політика використання, захисту й часу життя криптографічного ключа) |
| 43 | Політика анонімізації та псевдонімізації |
| 44 | Політика контролю доступу |
| 45 | Політика керування паролями  |
| 46 | Політика безпечної розробки  |
| 47 | План безперервності бізнесу та аварійного відновлення  |
| 48 | Заява про ознайомлення та прийняття документів системи управління інформаційною безпекою та конфіденційністю |
| 49 | Процедура управління інцидентами |
| 50 | Політика безпеки людських ресурсів |
|  | **Відносини з постачальниками, партнерами, Процесорами та****Контролерами** |
| 51 | Політика безпеки постачальника |
| 52 | Анкета відповідності Процесора персональних даних |
| 53 | Угода про обробку персональних даних (зразок на випадок, якщо є дозвіл Процесору PII від Контролера PII на обробку персональних даних) |
| 54 | Угода про обробку персональних даних (зразок на випадок, якщо є заборона Процесору PII від Контролера PII на обробку персональних даних) |
| 55 | Угода про обробку даних між Контролерами |
| 56 | Положення про безпеку для Постачальників і Партнерів |
| 57 | Заява про конфіденційність |
|  | **Процедури реагування та порядок повідомлення про події** |
| 58 | Процедура реагування на порушення даних і сповіщення  |
| 59 | Реєстр порушень даних (зразок) |
| 60 | Форма повідомлення про порушення даних для наглядового органу |
| 61 | Форма сповіщення суб’єктів даних про порушення даних |
| 62 | План реагування на інциденти (додаток: форма збору інцидентів) |
|  | **Навчання та підвищення обізнаності** |
| 63 | План навчання та інформування  |
|  | **Внутрішній аудит** |
| 64 | Процедура внутрішнього аудиту |
| 65 | Додаток 1 – Річна програма внутрішнього аудиту (зразок) |
| 66 | Додаток 2 – Звіт внутрішнього аудиту (зразок) |
| 67 | Додаток 3 – Перелік контролів внутрішнього аудиту відповідно до вимог ДСТУ ISO 27001:2023 |
|  | **Огляд з боку керівництва** |
| 68 | Звіт про вимірювання (зразок) |
| 69 | Протокол огляду з боку керівництва (зразок) |
|  | **Корегуючи дії** |
| 70 | Процедура коригуючих дій |
| 71 | Додаток – Форма коригувальних дій |
|  | **Управління правами суб'єкта персональних даних (зразки документів)** |
| 72 | Форма згоди суб'єкта даних |
| 73 | Відкликання згоди суб'єкта даних |
| 74 | Процедура запиту доступу суб'єкта даних |
| 75 | Форма запиту на доступ суб'єкта даних |
| 76 | Форма розкриття суб'єкта даних |
| 77 | Запит на підтвердження повноважень |
| 78 | Підтвердження запиту на доступ суб'єкта даних |
| 79 | Підтвердження запиту прав суб'єкта даних |
| 80 | Відхилення необґрунтованого/надмірного запиту |
| 81 | Підтвердження для закриття DSAR |
| 82 | Відповідь на запит доступу суб'єкта даних |
| 83 | Супровідний лист до відповіді на портативність |
| 84 | Відповідь на виправлення запиту даних |
| 85 | Відповідь на відкликання/обмеження згодиЗапит (відхилено) |
| 86 | Відповідь на відкликання/обмеження згодиЗапит (прийнято) |
| 87 | Відповідь на обробкуЗапит/скарга на обмеження (відхилено) |
| 88 | Відповідь на запит/скаргу щодо обмеження обробки(Прийнято) |
| 89 | Відповідь на автоматизоване прийняття/обмеженняОбробка (відхилено) |
| 90 | Відповідь на автоматизоване прийняття/обмеженняОбробки (прийнята) |
| 91 | Підтвердження на стирання даних |

**Проведення сертифікації телекомунікаційного обладнання,** що включає оцінку відповідності та сертифікації одного маршрутизатору (комутатору) та одного персонального комп’ютеру, а саме:

* аналіз наявності технічної, експлуатаційної документації на технічні засоби електронних комунікацій та проведення експертизи наданої документації на відповідність нормативним документам, які діють в Україні;
* аналіз наявності типових рядів у партії продукції, відбору та ідентифікації зразків технічних засобів електронних комунікацій для проведення сертифікаційних випробувань;
* проведення робіт з оцінки відповідності зразків технічних засобів електронних комунікацій вимогам до електробезпеки, електромагнітної сумісності та технічних характеристик. Випробування на відповідність мережевих протоколів нормативним документам ITU-T Y.1001, X.602 (RFC), електричних та оптичних параметрів мережевих на відповідність ДСТУ ISO/IEC/IEEE 8802-3:2015: - Ethernet 10/100/1000BASE-T (протоколи IP, TCP, UDP, ARP, ICMP, IGMPv2, SSH, RIPv1/v2; - IGMPv3, OSPF, SNMP, STP, MSTP, RSTP, xxx);
* проведення випробувань радіомодуля (інтерфейс передачі даних 802.11 a/b/g/n/ac та Bluetooth) в складі персонального комп’ютеру обладнання згідно ДСТУ ETSI EN 300 328:2017, ДСТУ ETSI EN 302 502:2016.

*Результатом є*: сертифікат відповідності або висновок про невідповідність технічних засобів електронних комунікацій, що надається акредитованим органом сертифікації.

**ЗАМОВНИК: ВИКОНАВЕЦЬ:**

**Виконавчий комітет**

**Криворізької міської ради**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_/\_\_\_\_\_\_\_\_\_**

# Додаток 2

# до Договору від \_\_\_\_\_\_\_\_\_ №\_\_\_\_

**К А Л Ь К У Л Я Ц І Я**

кошторисної вартості Послуги

ДК 021:2015:72220000-3, Консультаційні послуги з питань систем та з технічних питань  (консультаційні послуги щодо створення системи управління інформаційною безпекою та конфіденційністю у відповідності до вимог ДСТУ ISO/IEC 27001:2023, ДСТУ ISO/IEC 27701:2022 та сертифікації телекомунікаційного обладнання)

|  |  |  |
| --- | --- | --- |
| № | Статті витрат | Витрати, грн |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
| Всього |  |

**ЗАМОВНИК: ВИКОНАВЕЦЬ:**

**Виконавчий комітет**

**Криворізької міської ради**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_/\_\_\_\_\_\_\_\_\_**