*ЗАТВЕРДЖЕНО*

 *Рішення виконкому міської ради*

*25.07.2025 №938*

***ПОЛІТИКА БЕЗПЕКИ ПОСТАЧАЛЬНИКА***

***ВИКОНАВЧОГО КОМІТЕТУ КРИВОРІЗЬКОЇ МІСЬКОЇ РАДИ***

#### *1. Загальні положення*

1.1. Політика безпеки постачальника виконавчого комітету Криворізької міської ради (надалі – Політика) є документом для визначення основних правил безпеки взаємовідносин з постачальниками в межах безпеки ланцюга постачання програмного забезпечення (надалі – ПЗ), послуг/сервісів, обладнання до Єдиної інформаційної системи міста Кривий Ріг (надалі – ЄІС).

1.2. Політика має мету забезпечити:

1.2.1 процес придбання та підтримки ПЗ згідно з вимогами чинного законодавства та внутрішніх документів з питань інформаційної безпеки (надалі – ІБ) виконкому міської ради;

1.2.2 дотримання її вимог на всіх етапах життєвого циклу ПЗ у межах області дії системи управління інформаційною безпекою (надалі – СУІБ);

1.2.3 мінімізацію ризиків, пов’язаних з придбанням, постачанням і впровадженням ПЗ/послуг/сервісів/обладнання та інших компонентів в складі ЄІС у межах дії СУІБ.

1.3. Політика розроблена з метою впровадження заходів з розробки/модернізації/упровадження/поліпшення ПЗ із застосуванням ризикорієнтованого підходу на всіх етапах життєвого циклу СУІБ.

1.4. Політика застосовується до інформаційної діяльності (уключаючи дії, які можуть вплинути на обробку персональних даних) виконкому міської ради в області дії СУІБ:

1.4.1 усіх робочих процесів та інформації, що обробляє виконком міської ради;

1.4.2 усіх мереж, пристроїв та засобів обробки інформації, якими володіють або користуються посадові особи, підрядники, консультанти, постачальники, партнери та інші користувачі, пов’язані з діяльністю виконкому міської ради або іншими особами, які використовують або отримують доступ до сервісів у межах області дії СУІБ.

1.5. Політика застосовується до всіх постачальників і партнерів, що мають можливість впливати на конфіденційність, цілісність і доступність інформації, яка оброблюється у виконкомі міської ради в межах області дії СУІБ.

1.6. Політика розроблена відповідно до вимог чинного законодавства України, міжнародних стандартів та нормативно-правових актів, що регламентують сферу інформаційної безпеки, а саме: ДСТУ ISO/IEC 27001:2023 (ISO/IEC 27001:2022, IDT) «Інформаційна безпека, кібербезпека та захист конфіденційності. Системи керування інформаційною безпекою. Вимоги», ДСТУ ISO/IEC 27002:2023 (ISO/IEC 27002:2022, IDT) «Інформаційна безпека, кібербезпека та захист конфіденційності. Засоби контролювання інформаційної безпеки», ДСТУ ISO/IEC 27701:2022 (ISO/IEC 27701:2019, IDT) «Методи безпеки. Розширення до ISO/IEC 27001 та ISO/IEC 27002 для керування конфіденційною інформацією. Вимоги та настанови», Регламенту Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року про захист фізичних осіб у зв’язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄC (Загального регламенту про захист даних) (надалі – GDPR), Наказу Адміністрації ДержСпецзв’язку України від 06 жовтня 2021 року №601 «Про затвердження Методичних рекомендацій щодо підвищення рівня кіберзахисту критичної інформаційної інфраструктури», зі змінами, Стандарту інформаційної безпеки NIST Special Publication 800-53 Revision 5 «Security and Privacy Controlsfor Information Systems and Organizations», Структури кібербезпеки The NIST Cybersecurity Framework (CSF) 2.0, політик, процедур і технічних заходів: D4.1-СУІБ «Політика інформаційної безпеки», D14.9-СУІБ «Політика управління змінами», D10-СУІБ «Методологія оцінки та обробки ризиків», D14.10-СУІБ «Політика резервного копіювання», D14.11-СУІБ «Політика утилізації та знищення», D14.14-СУІБ «Політика контролю доступу», D14.16-СУІБ «Політика безпечної розробки».

####

#### *2. Терміни, визначення та скорочення*

2.1. Заявник – це суб’єкт PII, який за допомогою сервісів підсистеми «WebПортал» подає запит (електронне звернення) до повноважних органів виконкому міської ради з метою отримання адміністративних, інших публічних послуг, у тому числі з дозвільних питань, видачі документів дозвільного характеру, голосування за електронні петиції та подання скарг.

2.2. Суб’єкт PII – фізична особа, PII якої обробляються в межах її згоди та якої стосується ідентифікаційна інформація в межах визначеної мети обробки PII, що встановлює склад цих PII та процедури їх обробки, якщо інше не визначено законом.\*

2.3. Суб’єкти ЄІС – Криворізька міська рада, її виконавчі органи, підприємства, установи, організації, заклади комунальної власності міста, структурні підрозділи районних у місті рад, що користуються підсистемами ЄІС та обробляють інформацію для реалізації наданих повноважень.

2.4. Актив – активом є все, що має цінність для виконкому міської ради й потребує захисту [інформаційний актив, апаратне забезпечення, програмне забезпечення, інфраструктура, мережа розповсюдження інформації, посадові особи, сервіси, технології та ресурси (фінансові, технічні, адміністративні, організаційні) для забезпечення інформаційної діяльності, нематеріальні активи (імідж, довіра, сертифікати відповідності, ліцензії тощо)].

2.5. Власник активу – відповідальна посадова особа або відділи, управління інші виконавчі органи міської ради, у розпорядженні та/або користуванні, та/або розробці, та/або підтримці яких перебуває актив, що може впливати на інформаційну безпеку (надалі − ІБ) та кібербезпеку.\*\*

2.6. Інформаційний актив (надалі − ІА) – це сукупність відомостей (інформації у фізичній або електронній формі), що представляє цінність для виконкому міської ради, а також будь-яка інформаційна система обробки, обміну чи фізичного місця зберігання інформації.

2.7. ЄІС – багатофункціональна інтегрована автоматизована система, що безпосередньо забезпечує реалізацію функцій її суб’єктів, інформаційну підтримку та супроводження їх діяльності й становить сукупність взаємопов’язаних функціональних підсистем, програмно-інформаційних комплексів, комп’ютерних програм, програмно-технічних та технічних засобів телекомунікації, які забезпечують логічне поєднання визначених інформаційних ресурсів, обробку й захист інформації, внутрішню та зовнішню інформаційну взаємодію.

2.8. Chief Executive Officer ( надалі – CEO) – власник і розпорядник СУІБ.

2.9. Chief Security Officer (надалі – CSO) – відповідальний за РІІ, який відповідає за керування процесом організації безпеки у виконкомі міської ради, включаючи фізичну безпеку, ІБ, кібербезпеку та інші види безпеки в межах сфери застосування СУІБ.

2.10. Chief Information Security Officer (надалі − CISO) − відповідальний за розробку та впровадження політик і процедур ІБ, управління ризиками, забезпечення кібербезпеки, реагування на інциденти, підвищення обізнаності працівників та контроль за дотриманням законодавства у сфері захисту інформаційних систем і даних.

2.11. Data Protection Officer (надалі − DPO) − відповідальний за захист персональних даних (надалі – PII) у виконкомі міської ради, відповідає за організацію роботи, пов’язаної із захистом РІІ у процесі інформаційної діяльності виконкому в межах області дії СУІБ.

2.12. PII – персональні дані.

2.13. Зацікавлені сторони – це фізичні або юридичні особи, які можуть впливати або на яких може вплинути інформаційна діяльність виконкому міської ради. Зацікавленими сторонами вважаються:

2.13.1 органи державної влади України та за кордоном, у тому числі регуляторний орган, що здійснює державне регулювання у сферах енергетики та комунальних послуг;

2.13.2 органи місцевого самоврядування;

2.13.3 суспільство, громадські організації, міжнародні організації, міжнародні фінансові інституції, медіа, ділові, експертні та галузеві об’єднання, компанії енергетичного чи суміжних секторів економіки, дипломатичні кола тощо;

2.13.4 банки, інвестори, рейтингові агентства;

2.13.5 суб’єкти PII, процесори PII, підпроцесори PII, співконтролери PII, акціонери/власники бізнесу;

2.13.6 інші учасники інформаційного обміну, постачальники послуг/сервісів (у тому числі хмарних), провайдери та партнери, постачальники баз даних.

2.14. Третя сторона – це фізична або юридична особа, що може вплинути на ІБ та безперервність процесів. У контексті СУІБ третя сторона може не мати створений та зареєстрований акаунт у межах області дії СУІБ. Це можуть бути члени сімей посадових осіб, суб’єктів PII, процесорів PII, підпроцесорів PII, співконтролерів PII, екстрені служби, консультанти (включаючи юристів, податкових консультантів, консультантів з питань праці тощо), які можуть мати вплив на ІБ в межах області дії СУІБ.

2.15. Контролер PII – фізична або юридична особа, державний орган, агентство або будь–який інший орган, що самостійно чи спільно з іншими визначає цілі та засоби обробки PII.

2.16. Користувачі ЄІС – фізичні особи та юридичні особи, уповноважені посадові особи виконкому міської ради, уповноважені посадові особи суб’єктів ЄІС, яким у встановленому порядку надано відповідні права доступу до інформації в підсистемах ЄІС.

2.17. Chief Legal Officer (надалі – CLO) – керівник юридичного підрозділу.

2.18. Incident Response Team (надалі – IRT) – група реагування на інциденти.

2.19. Chief Human Resources Officer (надалі – CHRO) – відповідальна особа за кадрову політику.

2.20. CFO (Chief Financial Officer) – керівник підрозділу, що відповідає за фінансове забезпечення.

2.21. Інформаційно-комунікаційна система (надалі – ІКС) – до складу якої належить комплекс апаратних, програмних, апаратно–програмних (фізичних та/або віртуальних) телекомунікаційних засобів, призначених для маршрутизації, комутації, зберігання, приймання, передавання інформації між кінцевим обладнанням ІКС у межах виконання цілей виконкому міської ради.

#### *3. Відносини з постачальниками та партнерами*

3.1. Політика визначає вимоги щодо пом’якшення ризиків, пов’язаних з доступом постачальника до активів СУІБ. Детальна інформація та ризики безпеки, пов'язані з постачальниками й партнерами, визначаються в процесі оцінки ризиків, які врегульовано в D10-СУІБ «Методологія оцінки та обробки ризиків». У ході оцінки ризику, особливу увагу слід приділяти визначенню ризиків, пов'язаних з інформаційними та комунікаційними технологіями, а також ризиків, пов'язаних з ланцюгами поставок продукції (послуг/сервісів/обладнання/ПЗ тощо).

3.2. CSO ухвалює рішення про необхідність додаткової оцінки ризиків, пов'язаних з окремими постачальниками або партнерами.

3.3. Виконком міської ради гарантує, що потенційні ризики, пов’язані з роз-голошенням конфіденційних даних, ідентифікуються, документуються та роз-глядаються відповідно до Політики. Управління ризиками має невід’ємну роль на стратегічному та тактичному рівнях. Метою Політики для партнерів, зацікавлених і третіх сторін є забезпечення того, щоб партнерства та послуги досягали цілей і завдань інформаційної діяльності та відповідали вимогам СУІБ щодо ІБ.

3.4. Виконком міської ради без попередньої оцінки ризиків не передає конфіденційні дані зацікавленим та третім особам:

3.4.1 що можуть мати вплив на інформаційну діяльність виконкому міської ради;

3.4.2 оформлення письмової угоди про нерозголошення конфіденційної інформації;

3.4.3 описи робіт або угоди про надання послуг, у яких описуються очікувані рівні обслуговування та будь-які конкретні вимоги до ІБ.

3.5. Усі сторони, дотичні до інформаційної діяльності виконкому міської ради, мають підтримувати належний організаційний і технічний контроль заходів захисту ІА згідно з Політикою.

3.6. Виконком міської ради проводить оцінку ефективності СУІБ зацікавленим та третім сторонам, що в процесі інформаційної діяльності можуть отримати конфіденційні дані, які зацікавлені та треті сторони обробляють або зберігають у власних ІКС.

3.7. Під час оцінки виконком міської ради розглядає зацікавленими та третіми сторони наявність таких заходів та засобів ІБ відповідно до вимог ISO 27001:

3.7.1 Політика інформаційної безпеки: зацікавлені та треті сторони повинні дотримуватися політик ІБ, що підтримуються і переглядаються їх керівництвом

3.7.2 оцінка та обробка ризиків: зацікавлені та треті сторони повинні підтримувати програми, що визначають, оцінюють і керують інформаційними та тех-нологічними ризиками;

3.7.3 безпека операцій: зацікавлені та треті сторони повинні впроваджувати обґрунтовані практики та процедури, призначені для організації безпеки операцій щодо виконання вимог ІБ у межах діючого договору, що можуть включати:

3.7.3.1 технічні випробування;

3.7.3.2 захист від шкідливого ПЗ;

3.7.3.3 захист і управління мережею;

3.7.3.4 управління технічними вразливостями;

3.7.3.5 ведення журналів (логи) та моніторинг;

3.7.3.6 реагування на інциденти;

3.7.3.7 виконання політики криптографії;

3.7.3.8 планування безперервності роботи.

3.7.4 управління доступом: зацікавлені та треті сторони повинні підтримувати правила контролю доступу;

3.7.5 розробка безпечної системи: зацікавлені та треті сторони повинні підтримувати безпечну програму розробки, що відповідає найкращим практикам розробки галузевого ПЗ та систем, включаючи оцінку ризиків, формальне керування змінами, стандарти коду, перевірку та тестування коду;

3.7.6 фізична та екологічна безпека: якщо зацікавлені та треті сторони зберігають або обробляють конфіденційні дані, їх засоби контролю фізичної та нав-колишньої безпеки мають відповідати вимогам фізичної безпеки згідно з політиками ІБ;

3.7.7 людські ресурси: зацікавлені та треті сторони повинні підтримувати політику й процеси щодо кадрів, що включають перевірку кримінального минулого для будь-яких працівників або підрядників, які мають доступ до конфіденційної інформації;

3.7.8 відповідність вимогам і праву: виконком міської ради враховує всі від-повідні норми та закони під час оцінки постачальників, що матимуть доступ, зберігатимуть, оброблятимуть або передаватимуть конфіденційні дані.

3.8. СЕО ухвалює рішення про необхідність виконання комплексної експертизи окремих постачальників і партнерів та які методи слід використовувати.

3.9. Для всіх постачальників послуг, які мають доступ до конфіденційних даних, систем або мереж виконкому міської ради, необхідно провести належну перевірку перед наданням доступу або залученням до обробки інформації з обмеженим доступом. Необхідно зберігати актуальну інформацію про те, які нормативні або сертифікаційні вимоги висовуються до кожного постачальника послуг. Застосовні нормативні або сертифікаційні вимоги можуть включати ISO 27001, ISO 27701, GDPR або інші стандарти чи правила.

3.10. Оцінки зацікавленої або третьої сторони враховують такі критерії:

3.10.1 захист даних клієнтів, організаційних записів, зберігання та видалення записів;

3.10.2 конфіденційність РІІ.

3.11. CSO вирішує необхідність проведення перевірки даних для окремих постачальників і партнерів і, якщо так, вибирає один з таких методів – досвід інших клієнтів, кредитна історія, аудит на місці.

3.12. У випадках, коли в системі постачальника обробляються РІІ, DPO несе відповідальність за те, щоб потенційні або існуючі постачальники заповнили анкету відповідності щодо захисту РІІ (зразок наведений у D15.2-СУІБ «Опитувальник відповідності Процесора PII»). Указана в анкеті відповідності постачальником інформація дає змогу оцінити поточний рівень його готовності як процесора РІІ захисту PII відповідно до вимог ДСТУ ISO/IEC 27701 та GDPR. Зібрана інформація, використовується для ухвалення рішення про співпрацю з потенційним постачальником, а також необхідність унесення покращень, що запропоновані постачальниками.

3.13. CSO відповідає за визначення положень ІБ, що мають бути включені в договір з постачальником. DPO відповідає за визначення положень із захисту PII, що мають бути включені в договір з постачальником.

3.14. Рішення про включення відповідного положення до умов договору, базується на результатах оцінки й обробки ризиків, пов’язаних з отриманням послуг/сервісів/обладнання від постачальника. Положення, що передбачають конфіденційність і повернення активів після розірвання договору, є обов'язковими. Крім того, у договорах мають бути відомості, що чітко вказують повноваження виконкому міської ради щодо контролю надійності, якості, повноти та своєчасності поставки продуктів і послуг.

3.15. СЕО за поданням CSO ухвалює рішення про необхідність окремим працівникам постачальників/партнерів підписати заяви про конфіденційність при роботі або достатньо загальної угоди між виконкомом міської ради та постачальником.

3.16. СЕО за поданням CSO ухвалює рішення про відповідального за конкретного постачальника або партнера щодо виконання умов договору.

3.17. Для постачальників, що надають послуги з обробки РІІ, DPO несе відповідальність за підписання угоди, яка має включати вимоги національного та міжнародного законодавства (нормативно-правових актів, згоду на виконання яких надала Верховна Рада України) щодо безпечної обробки РІІ [більш детальна інформація про варіанти угод викладена в документах D15.3-15.4 СУІБ «Угода про обробку персональних даних» (зразок на випадок, якщо є дозвіл процесору РІІ від контролера РІІ на обробку РІІ), D15.4-СУІБ «Угода про обробку персональних даних» (зразок на випадок, якщо є заборона процесору РІІ від контролера РІІ на обробку РІІ)].

3.18. Для інших постачальників CSO несе відповідальність за ухвалення рішень про положення ІБ, що включені в контракт з постачальником. Рішення ґрунтується на результатах оцінки та обробки ризику.

3.19. Відповідні вимоги до ІБ встановлюються та узгоджуються з кожним постачальником, що отримує доступ до обробки, зберігання чи передачі конфіденційних даних або надання компонентів фізичної чи віртуальної ІТ-інфраструктури для виконкому міської ради.

3.20. З усіма постачальниками послуг, що можуть отримати доступ до виробничих систем або впливати на безпеку виробничого середовища виконкому міської ради, укладаються письмові угоди, що включають підтвердження постачальником послуг їх відповідальності за конфіденційність даних, а також будь-які зобов’язання стосовно виконання та забезпечення контролю цілісності, доступності та/або конфіденційності, якими вони керують, щоб відповідати стандартам і вимогам, установленим виконкомом міської ради відповідно до політик ІБ.

3.21. Виконком міської ради розглядає та оцінює ризики, пов’язані з постачальниками та ланцюгом постачання технологій. Якщо це виправдано, угоди з постачальниками включають вимоги стосовно усунення відповідних ризиків ІБ, пов’язаних з послугами інформаційно-комунікаційних технологій і ланцюгом постачання продукції.

3.22. У договорах з постачальниками обов'язковими є такі пункти:

3.22.1 збереження конфіденційності інформації;

3.22.2 повернення активів після розірвання або закінчення договору;

3.22.3 як інформація про загрози/вразливості/ризики/інциденти передається між постачальником і виконкомом міської ради;

3.22.4 забезпечення надійної доставки продуктів і послуг, що особливо важливо для постачальників «хмарних послуг»;

3.22.5 перелік (посада, прізвище, ім’я, по батькові) та контактні дані відповідальних від постачальника та виконкому міської ради, а саме: CSO, DPO, власник договору, адміністратор IRT.

3.23. Перелік базових положень наведено в D15.8-СУІБ «Положення про безпеку для постачальників і партнерів».

3.24. Власник договору ухвалює рішення про працівників постачальників і партнерів, що потребують обізнаності й навчання з ІБ у межах сфери застосування СУІБ.

3.25. CSO має забезпечити проведення навчання та підвищення обізнаності цих працівників у сфері ІБ та кіберзахисту.

3.26. DPO має забезпечити проведення навчання та підвищення обізнаності цих працівників у сфері захисту PII.

3.27. Власник договору регулярно перевіряє і контролює рівень обслуговування та виконання вимог ІБ постачальниками або партнерами, перевіряє звіти та записи, створені постачальниками/партнерами. Власник договору контролює своєчасність проведення аудиту ІБ із залученням внутрішніх аудиторів виконкому міської ради, постачальників або партнерів, принаймні один раз на рік.

3.28. Аудит проводиться внутрішніми аудиторами виконкому міської ради за процедурою, указаною у D18-СУІБ «Процедура внутрішнього аудиту».

3.29. Обсяг аудиту визначає CSO або відповідальний керівник підрозділу внутрішнього аудиту за поданням власника договору та внутрішніх аудиторів виконкому міської ради, що готують плани аудиторських тестів з визначенням таких заходів:

3.29.1 інтерв’ю з керівним складом постачальника;

3.29.2 директивне інтерв’ю з уповноваженими особами постачальника: CSO, CFO, CHRO, CLO, CISO, CIO, DPO;

3.29.3 метод вибірки та реалізація плану вибірки з урахуванням ризиків та суттєвості систем, робочих процесів, ІА.

3.30. Усі порушення ІБ, пов'язані з постачальниками/партнерами, негайно доводяться до CSO. CSO відповідає за щорічне планування та організацію проведення внутрішніх аудитів ІБ.

3.31. Власник договору пропонує CEO змінити або розірвати договір у разі порушення вимог ІБ Постачальником. За необхідності CSO за рішенням CEO виконує нову оцінку ризику, перш ніж ці зміни будуть прийняті.

3.32. При зміні або розірванні договору, права доступу для працівників партнерів/постачальників видаляються відповідно до Політики управління доступом.

3.33. Якщо договір розірваний або змінений, власник договору переконує-ться та звітує на адресу CEO/CSO, що все обладнання, ПЗ та інформація в електронному чи паперовому вигляді були повернені.

*\*Залежно від юрисдикції та конкретного законодавства про захист персональних даних і конфіденційності фрази «суб’єкт даних» або «суб’єкт PII» або «власник ідентифікаційної інформації» є синонімом фрази «суб’єкт PII».*

*\*\*Термін «Власник» ідентифікує посадових осіб, відділи, управління, інші виконавчі органи міської ради, для яких установлено відповідальність щодо здійснення контролю за створенням, розвитком, підтримкою, використанням безпеки активів та ресурсів СУІБ. Термін «Власник» не означає, що особа дійсно має право власності на активи/ресурс/ризик СУІБ.*

***Керуюча справами виконкому Олена ШОВГЕЛЯ***