*ЗАТВЕРДЖЕНО*

 *Рішення виконкому міської ради*

*25.07.2025 №938*

***ПОЛІТИКА БЕЗПЕКИ ЛЮДСЬКИХ РЕСУРСІВ***

***ВИКОНАВЧОГО КОМІТЕТУ КРИВОРІЗЬКОЇ МІСЬКОЇ РАДИ***

#### *1. Загальні положення*

1.1. Політика безпеки людських ресурсів виконавчого комітету Криворізької міської ради (надалі – Політика) є документом, що встановлює порядок керування людськими ресурсами в процесі здійснення інформаційної діяльності в межах області дії системи управління інформаційною безпекою (надалі – СУІБ).

1.2. Політика розроблена з метою впровадження заходів з управління людським ресурсами із застосуванням ризикорієнтованого підходу на всіх етапах життєвого циклу СУІБ.

1.3. Політика розроблена відповідно до вимог чинного законодавства України, міжнародних стандартів та нормативно-правових актів, що регламентують сферу інформаційної безпеки, а саме: Законів України «Про інформацію», «Про захист персональних даних», Про захист інформації в інформаційно-комунікаційних системах»; 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», D14.14-СУІБ «Політика контролю доступу».

#### *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. PII – персональні дані.

2.3. 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.\*

2.4. 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. Єдина інформаційна система міста Кривий Ріг (надалі – 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.

2.7. Суб’єкти ЄІС – Криворізька міська рада, її виконавчі органи, підприємства, установи, організації, заклади комунальної власності міста, районні в місті ради, що користуються підсистемами ЄІС та обробляють інформацію для реалізації наданих повноважень.

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

2.9. Chief Security Officer (надалі – CSO) – відповідальний за ІБ, 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. Зацікавлені сторони – це фізичні або юридичні особи, які можуть впливати або на яких може вплинути інформаційна діяльність виконкому міської ради. Зацікавленими сторонами вважаються:

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

2.10.2 органи місцевого самоврядування;

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

2.10.4 банки, інвестори, рейтингові агентства;

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

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

2.11. 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, спів-контролерів PII, екстрені служби, консультанти (включаючи юристів, податкових консультантів, консультантів з питань праці тощо), які можуть мати вплив на ІБ в межах області дії СУІБ.

2.12. 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.

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

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

#### *3. Керівництво з упровадження заходів захисту*

3.1. Перевірка посадових осіб виконкому міської ради проводиться відповідно до законодавчих актів України з урахуванням захисту PII під час їх обробки у процесі скринінгу, та має бути пропорційною вимогам ІБ й обмежень, що виникають з приводу доступу посадових осіб (або потенційних посадових осіб – кандидатів) до інформації з урахуванням її критичності, рівня конфіденційності та ризиків ІБ.

3.2. Перевірка включає наявність кримінальних злочинів, якщо це не заборонено законодавством України. Усі особи, які в процесі інформаційної діяльності будуть мати або мають технічні привілеї чи адміністративний доступ до виробничих систем ЄІС, підлягають обов’язковій перевірці, залежно від рівня їх доступу та уявлення про ризики ІБ.

3.3. Навички та компетентність посадових осіб виконкому міської ради й підрядників власника СУІБ оцінюються уповноваженими особами кадрового забезпечення в рамках процесу найму на роботу або під час обрання підрядника. Обов'язкові навички й компетентності мають бути вказані в описах посад і запитаннях на вакансії. Оцінка компетентності може включати перевірку рекомендацій, освіти й сертифікатів, технічне тестування та співбесіди. Усі посадові особи проходитимуть щорічний огляд ефективності, що включатиме оцінку роботи, компетентності в певній ролі, дотримання політик, процедур, правил СУІБ та кодексу поведінки, а також досягнення конкретних цілей у своєї ролі.

3.4. Наприкінці року (до 15 грудня поточного року) CHRO звітує перед CEO про відповідність кваліфікації та компетенції привілейованих користувачів і користувачів з адміністративними ролями.

3.5. CSO та CHRO є відповідальними за планування заходів з підвищення кваліфікації користувачів, що мають роль у межах СУІБ, та підвищення стану їх обізнаності в галузі ІБ.

3.6. Політики СУІБ та обов'язки з ІБ доводяться посадовим особам виконкому міської ради і стороннім особам під час прийому на роботу чи залучення до співпраці у межах їх повноважень та правил розмежування доступу. Посадові особи та зацікавлені особи з доступом до інформаційних активів СУІБ чи суб’єктів PII, підписують відповідну угоду про нерозголошення конфіденційної інформації. Угода вказує відповідальність за дотримання політик з ІБ. Посадові особи та відповідні зацікавлені особи повинні дотримуватися всіх політик ІБ виконкому міської ради.

3.7. Виконком міської ради відповідає за те, щоб політики та процедури з ІБ переглядалися щорічно, розповсюджувалися та були доступні, а посадові особи, які мають певну роль у СУІБ, та підрядники дотримувалися цих політик і процедур протягом терміну їх роботи чи співпраці. Щорічний огляд політик включає перегляд будь-яких пов'язаних чи зазначених процедур, стандартів чи вказівок. Виконком міської ради забезпечує повідомлення про відповідальність з ІБ особам через письмові описи посад, політики СУІБ чи іншим документованим методом, який періодично (не рідше одного разу на рік) оновлюється/переглядається та зберігається. Відповідність політикам та процедурам ІБ й виконання обов'язків з ІБ оцінюється в рамках процесу огляду продуктивності, де це застосовано.

3.8. Усі посадові особи та зацікавлені особи з адміністративним або привілейованим технічним доступом до виробничих систем ЄІС проходять інструктаж уповноважених осіб виконкому міської ради з ІБ на момент прийому на роботу та щорічно після цього, а також у процесі виконання посадових обов’язків періодичні навчання (курси підвищення кваліфікації, семінари, конференції, заняття з ІБ тощо) відповідно до планів. Виконком міської ради відстежує завершення навчання і впроваджує заходи для забезпечення відповідності Політиці. Посадові особи та підрядники мають бути обізнані з відповідними політиками та процедурами ІБ до початку виконання завдань у межах повноважень.

3.9. Уживаються заходи, включно з інформуванням про інциденти, щоб відповідні особи знали про можливі наслідки (наприклад, юридичні наслідки, шкода репутації) для посадової особи (наприклад, дисциплінарні наслідки) та для суб’єкта РІІ (наприклад, фізичні, матеріальні та емоційні наслідки) порушення правил і процедур конфіденційності або безпеки, особливо тих, що стосуються поводження з РІІ.

*\*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***