*ЗАТВЕРДЖЕНО*

 *Рішення виконкому міської ради*

*25.07.2025 №938*

***ПОЛІТИКА ЗБЕРЕЖЕННЯ ДАНИХ***

***ВИКОНАВЧОГО КОМІТЕТУ КРИВОРІЗЬКОЇ МІСЬКОЇ РАДИ***

#### *1. Загальні положення*

1.1. Політика збереження даних виконавчого комітету Криворізької міської ради (надалі – Політика збереження даних) установлює обов'язкові строки зберігання для певних категорій персональних даних (надалі - PII) та мінімальні вимоги, які слід застосовувати при знищенні певної інформації в межах виконкому міської ради.

1.2. Політика збереження даних застосовується до всіх відділів, управлінь, інших виконавчих органів міської ради, процесів і систем в усіх країнах, у яких виконком міської ради здійснює інформаційну діяльність пов’язану з PII та має відносини з третіми сторонами як контролер PII або процесор PII.

1.3. Політика збереження даних застосовується до всіх посадових осіб, підрядників, консультантів, радників або постачальників послуг виконкому міської ради, що можуть збирати, обробляти або мати доступ до PII.

1.4. Політика збереження даних застосовується до всієї інформації, що використовується у виконкомі міської ради. Приклади документів включають:

1.4.1 електронну пошту;

1.4.2 документи на папері;

1.4.3 документи в електронному вигляді;

1.4.4 відео- та аудіозаписи;

1.4.5 інші дані, створені системами контролю за доступом тощо.

1.5. Політика збереження даних 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), політик, процедур і технічних заходів: D2-СУІБ Порядок ідентифікації вимог; D4.1-СУІБ «Політика інформаційної безпеки»; D4.3-СУІБ «Політика захисту персональних даних посадових осіб»; D14.11-СУІБ «Політики утилізації та знищення».

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

2.1. 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)].

2.2. 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.\*

2.3. 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.

2.4. 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.

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

2.6. 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.

2.7. 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.

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

2.9. 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.

2.10. PII – персональні дані.

2.11. Chief Information Officer (надалі − CIO) − відповідальний за розробку та реалізацію стратегії цифрової трансформації міста, управління інформаційними системами та ресурсами, кібербезпеку.

2.12. 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.

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

#### *3. Правила зберігання інформації*

3.1. Виконком міської ради розробляє та підтримує графіки зберігання інформації, беручи до уваги вимогу зберігати PII не довше, ніж це необхідно. Такі графіки враховують законодавчі, нормативні та ділові вимоги. Якщо зберігання інформації суперечить законодавчим, нормативним та діловим вимогам, тоді приймається відповідне рішення (на основі оцінки ризику) та документується у відповідному графіку.

3.2. У разі, якщо для будь-якої категорії документів не визначено окремо в Політиці збереження даних і відсутні інші обов'язкові вимоги законодавчих актів, строк зберігання для такого документа вважатиметься 3 роки з дати його створення.

3.3. DPO у відповідності до законодавчих актів і згоди суб’єкта PII, створює графік зберігання PII та подає на затвердження СЕО.

3.4. Строк зберігання може бути подовжений у таких випадках:

3.4.1 проведення поточних розслідувань уповноваженими органами Європейського Союзу, Європейською асоціацією вільної торгівлі, України, якщо є ймовірність, що записи PII можуть знадобитися виконкому міської ради для підтвердження відповідності вимогам чинного законодавства;

3.4.2 використання правових засобів у судових справах або аналогічних судових процедурах, визнаних місцевим законодавством.

3.5. Ураховується можливість зносу (виходу з ладу) носіїв даних, що використовуються для архівування. ІА, що зберігається на носіях даних, доступний уповноваженим користувачам виконкому міської ради в межах визначеного строку зберігання PII (як стосовно інформаційного носія, так і щодо читабельності форматів). ІА на носіях зберігається з урахуванням протидії загрозам, які внаслідок майбутніх технологічних змін можуть призвести до втрати доступу до PII (наприклад: несумісність формату запису з форматом читання). Відповідальність за доступність до PII покладається на CISO, CIO та власника активу.

3.6. Дані знищуються відповідно до D14.11-СУІБ «Політика утилізації та знищення інформації».

3.7. DPO забезпечує, щоб кожна посадова особа виконкому міської ради та користувачі ІКС дотримувалися Політики збереження даних. Також на DPO покладено відповідальність за допомогу будь-якій посадовій особі, користувачу ІКС, суб’єкту PII у наданні роз’яснень запитів від місцевого чи урядового органу стосовно PII. Про будь-яку підозру щодо порушення Політики збереження даних, посадовим особам та користувачам ІКС необхідно негайно повідомити DPO та CSO. Усі випадки підозри в порушенні Політики збереження даних мають бути розслідувані й ужиті відповідні заходи.

3.8. Графік регулярного видалення: записи, які можуть знищуватися без дозволу DPO, CSO, CEO, якщо вони не підпадають під поточні правові або регуляторні дослідження, включають такі:

3.8.1 оголошення та повідомлення щоденних зустрічей та інших подій, включаючи прийняття та вибачення;

3.8.2 запити для отримання звичайної інформації;

3.8.3 бронювання внутрішніх зустрічей;

3.8.4 документи передачі, такі як листи, титульні сторінки факсів, електронні повідомлення, листівки, маршрутні листки, листи з вітанням та такого роду елементи, що містять документи виконкому міської ради, але не мають цінності;

3.8.5 повідомлення, що не містять інформації з обмеженим доступом;

3.8.6 застарілі списки адрес, списки розсилки тощо;

3.8.7 дублікати документів, такі як копії звичайної інформації, щоденні файли;

3.8.8 записи внутрішніх публікацій, які є застарілими;

3.8.9 застарілі каталоги постачальників, листівки та бюлетені від постачальників або інших зовнішніх організацій.

3.9. Під час видалення інформації потрібно враховувати:

3.9.1 якщо йде судовий процес або є інші юридичні підстави, дані можуть не підлягати видаленню, оскільки вони зберігаються як доказ;

3.9.2 політики СУІБ у яких визначені вимоги збереження/видалення даних.

*\*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***