*ЗАТВЕРДЖЕНО*

 *Рішення виконкому міської ради*

*25.07.2025 №938*

***ПОЛІТИКА УТИЛІЗАЦІЇ ТА ЗНИЩЕННЯ ІНФОРМАЦІЇ***

***ВИКОНАВЧОГО КОМІТЕТУ КРИВОРІЗЬКОЇ МІСЬКОЇ РАДИ***

#### *1. Загальні положення*

1.1. Політика утилізації та знищення інформації виконавчого комітету Криворізької міської ради (надалі – Політика утилізації та знищення) є документом, що забезпечує безпечне знищення або стирання інформації, яка зберігається на вмонтованих та з’ємних носіях інформації.

1.2. Політика утилізації та знищення застосовується до всієї області дії системи управління інформаційною безпекою (надалі – СУІБ), а саме:

1.2.1 усіх операційних процесів, програмних продуктів та їх налаштувань, інформації, що обробляється в Єдиній інформаційній системі міста Кривий Ріг (надалі – ЄІС);

1.2.2 усіх користувачів виконкому міської ради або інших дотичних сторін, які мають певні повноваження та отримують доступ до ЄІС у межах області дії СУІБ.

1.3. Політика утилізації та знищення 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 «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», рішень виконкому міської ради від 26.05.2021 №488 «Про впровадження Єдиної інформаційної системи міста Кривого Рогу»; 24.11.2021 №933 «Про затвердження Регламенту впровадження та визначення адміністратора Єдиної інформаційної системи міста Кривого Рогу», 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: D00DI-СУІБ «Порядок оформлення документів та контроль записів», D4.1-СУІБ «Політика інформаційної безпеки», D2.2-СУІБ

«Політика управління активами», D8.1-СУІБ «Положення щодо інвентаризації та обробки даних», D10-СУІБ «Методологія оцінки та обробки ризиків», D14.1-СУІБ «Політика ІТ-безпеки», D14.6-СУІБ «Політика класифікації інформації», D14.14-СУІБ «Політика контролю доступу», D14.10-СУІБ «Політика резервного копіювання», D14.12-СУІБ «Політика криптографії».

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

2.1. Критичні операційні процеси – операційні процеси діяльності виконкому міської ради, що визначені критичними щодо інформаційної безпеки за результатом їх оцінювання за такими критеріями: конфіденційність, цілісність, доступність.

2.2. 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)].

2.3. 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.\*

2.4. 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.

2.5. 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, що забезпечують логічне поєднання визначених інформаційних ресурсів, обробку й захист інформації, внутрішню та зовнішню інформаційну взаємодію.

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

2.7. 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.

2.8. Data Protection Officer (надалі − DPO) − відповідальний за захист персональних даних у виконкомі міської ради, відповідає за організацію роботи, пов’язаної із захистом персональних даних 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.

#### *3. Утилізація та знищення інформації та носіїв інформації*

3.1. Усі дані (ІА, уключаючи PII) та ліцензійне програмне забезпечення, які збережені на мобільному носії (наприклад, на CD, DVD, USB флеш-диску, карті пам'яті і т. ін., а також на папері) і на всьому обладнанні, що містить вбудовані носії інформації (наприклад, комп'ютери, мобільні телефони і т. ін.) видаляються з мобільного носія або обладнання перед повторним використанням чи перед утилізацією. Після виконання цієї процедури носії інформації мають бути утилізовані/знищені відповідною комісією виконкому міської ради, що створюється розпорядженням CEO (надалі – комісія).

3.2. Особа, відповідальна за видалення/руйнування даних та утилізацію/знищення носіїв, має повідомити відповідного власника активу про стирання/знищення даних.

3.3. Обладнання – носій інформації:

3.3.1 при внутрішньому переміщенні обладнання в межах виконкому міської ради відповідальна посадова особа виконує форматування носія перед виконанням інших регламентних робіт;

3.3.2 при зовнішньому переміщенні обладнання (коли обладнання передається за межі виконкому міської ради), відповідальним за перевірку й видалення даних з обладнання є власник активу;\*\*

3.3.3 видалення інформації з обмеженим доступом (надалі – ІзОД) виконанується з використанням надійних інструментів (багаторазове затирання/перезаписи «нулями» або знищення носія ІА методом спалення або фізичного руйнування, чи з використанням спеціальних програмних засобів, які гарантують неможливість відновлення ІА). Обрання засобів знищення обирає власник активу за згодою CSO чи CEO або комісією. Засоби знищення мають забезпечити унеможливлення встановлення ІзОД;

3.3.4 якщо процес видалення ІзОД на погляд CSO недостатньо безпечний, ураховуючи чутливість даних, то CSO сумісно з уповноваженим відділом, управлінням, іншим виконавчим органом міської ради порушує питання перед CEO про знищення обладнання, що має у своєму складі ІзОД.

3.4. Мобільні носії інформації:

3.4.1 при внутрішньому переміщенні матеріального носія інформації (нада-лі – МНІ) власник активу або окремо призначена розпорядженням CEO особа (адміністратор системи/підсистеми, адміністратор документів, відповідальний за облік та зберігання або комісія тощо) виконує його форматування;

3.4.2 при зовнішньому переміщенні МНІ (коли МНІ передається за межі виконкому міської ради), відповідальним за перевірку й видалення даних з МНІ є власник активу.\*\*\*

3.4.3 видалення ІзОД виконується з використанням надійних інструментів (багаторазове затирання/перезаписи «нулями» або знищення МНІ методом спалення чи фізичного руйнування або з використанням спеціальних програмних засобів, що гарантують неможливість відновлення ІА). Обрання засобів знищення обирає власник активу за згодою з CSO чи CEO, або комісією. Засоби знищення мають забезпечити унеможливлення встановлення ІзОД;

3.4.4 якщо процес видалення ІзОД на погляд CSO недостатньо безпечний, ураховуючи чутливість даних, то CSO сумісно з уповноваженим відділом, управлінням, іншим виконавчим органом міської ради порушує питання перед CEO про знищення МНІ, що містить ІзОД.

3.5. Інформація на папері:

3.5.1 посадові особи виконкому міської ради, які працюють з інформацією на папері, несуть відповідальність за її знищення. Інформація, викладена на папері, є паперовим документом;

3.5.2 паперові документи знищуються в шредері.

3.5.3 Відповідальним за знищення інформації на паперовому носії є власник активу.\*\*\*\*

3.6. Записи про знищення даних: документування факту проведеного знищення ІзОД має бути додане у формі позначки *«ІзОД відсутня, знищено ІзОД підтверджується Актом від\_\_\_\_\_№\_\_\_\_\_\_\_\_»* до усіх МНІ або обладнання, що передається у виконкомі міської ради або за його межами.\*\*\*\*\*

3.7. Носії ІзОД: обліковуються згідно з вимогами СУІБ D00DI-СУІБ «Порядок оформлення документів та контроль записів», D2.2-СУІБ «Політика управління активами користувачів», D8.1-СУІБ «Положення щодо інвентаризації та обробки дани». МНІ з ІзОД, повинні мати реквізити, установлені відповідно до вимог. МНІ з ІзОД, що не потрібні в подальшій роботі або вийшли з ладу, передаються для знищення до адміністратора документів. Знищення проводиться комісією, що створюється розпорядженням CEO.

3.8. Захищений носій ключової інформації (надалі – ЗНКІ): для роботи програмного IP-шифратора є обов’язковим використання ЗНКІ. Призначенням ЗНКІ забезпечується надійне зберігання ключових даних, що використовуються програмним шифратором. Облік ЗНКІ ведеться окремо від обліку МНІ з ІзОД та паперових носіїв. Знищення ЗНКІ з даними здійснюється комісією відповідно до документа «D14.12-СУІБ Політика криптографії». Журнал обліку повинен містити такі відомості:

3.8.1 назва засобу криптографічного захисту інформації (надалі – КЗІ) та його заводський номер;

3.8.2 тип носія ключової інформації та його обліковий номер;

3.8.3 акт організаційно-розпорядчого характеру щодо введення в експлуатацію засобів КЗІ;

3.8.4 дата взяття на облік засобів КЗІ та носіїв ключової інформації;

3.8.5 для програмних засобів КЗІ – інвентарні номери, на яких установлені програмні засоби КЗІ;

3.8.6 прізвище, ім’я, по батькові особи, відповідальної за облік засобів КЗІ та носіїв ключової інформації, підпис;

3.8.7 прізвище, ім’я по батькові особи, яка отримала засіб КЗІ та носії ключової інформації (дата, підпис);

3.8.8 відмітка про повернення засобу КЗІ та носіїв ключової інформації (дата, підпис відповідальної особи);

3.8.9 відмітка про знищення засобів КЗІ та носіїв ключової інформації (номер акта, дата, підпис відповідальної особи).

#### *4. Ролі та відповідальність*

4.1. CSO та DPO відповідають за супроводження процесу знищення інформації та здійснюють постійний контроль за ним.

4.2. Власник активу відповідає за виконання політик СУІБ стосовно правил обліку, зберігання, передачі, отримання, знищення та утилізації активів.

*\*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.*

*\*\*За розпорядженням CEO переміщення обладнання може відбуватися без згоди власника активу, при цьому розпорядженням CEO призначається комісія, яка виконує заходи відповідно до пункту 3.1. Політики утилізації та знищення.*

*\*\*\*За розпорядженням CEO переміщення МНІ може відбуватися без згоди власника активу, при цьому розпорядженням CEO призначається комісія, яка виконує заходи відповідно до пункту 3.1. Політики утилізації та знищення.*

*\*\*\*\*За розпорядженням CEO знищення паперового документа може відбуватися без згоди власника активу, при цьому розпорядженням CEO призначається комісія, яка виконує заходи відповідно до пункту 3.1. Політики утилізації та знищення.*

*\*\*\*\*\*Форму позначки слід розуміти як приклад. Форму та вміст можливо змінювати за рішенням CSO.*

***Керуюча справами виконкому Олена ШОВГЕЛЯ***