*ЗАТВЕРДЖЕНО*

 *Рішення виконкому міської ради*

*25.07.2025 №938*

***ПОЛІТИКА УПРАВЛІННЯ АКТИВАМИ***

***ВИКОНАВЧОГО КОМІТЕТУ КРИВОРІЗЬКОЇ МІСЬКОЇ РАДИ***

#### *1. Загальні положення*

1.1. Політика управління активами виконавчого комітету Криворізької міської ради (надалі – Політика управління активами) є документом, що визначає порядок ідентифікації активів виконкому Криворізької міської ради в межах області дії системи управління інформаційною безпекою (надалі – СУІБ) та встановлює відповідальність стосовно їх захисту.

1.2. Політика управління активами застосовується до всіх активів, якими володіє або керує виконком Криворізької міської ради в межах області дії СУІБ. Її основне призначення полягає в забезпеченні належного рівня захисту інформації відповідно до її важливості, режиму доступу та запобігання втраті активів СУІБ, несанкціонованому розголошенню, модифікації, видаленню або знищенню інформації, що обробляється у виконкомі міської ради.

1.3. Політика управління активами 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 доступ до публічної інформації», «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», 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 Controls for Information Systems and Organizations», «Структури кібербезпеки The NIST Cybersecurity Framework (CSF) 2.0», політик, процедур і технічних заходів: D4.1-СУІБ «Політика інформаційної безпеки», D4.6-СУІБ «Норми поведінки», D8.1-СУІБ «Положення щодо інвентаризації та обробки даних», D14.1-СУІБ «Політика ІТ-безпеки», D14.3-СУІБ «Політика мобільних пристроїв, віддаленої роботи та роботи з дому», D14.4-СУІБ «Політика щодо власного пристрою (BYOD)», D14.11-СУІБ «Політика утилізації та знищення», D14.14-СУІБ «Політика контролю доступу».

#### *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. Security Operations Center (надалі − SOC) − група інформаційної безпеки, що відповідає за моніторинг, виявлення, аналіз та реагування на інциденти кібербезпеки в реальному часі.

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

2.6. Chief Security Officer (надалі – CSO) – відповідальний за інформаційну безпеку, 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. 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 в межах області дії СУІБ.

2.8. Bring your own device (надалі − BYOD) – це IT-політика, згідно з якою посадовим особам дозволено або рекомендується використовувати особисті мобільні пристрої (телефони, планшети, ноутбуки) для доступу до даних і систем.

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. Сервіс–Деск – система реєстрації запитів.

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

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

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

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

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

2.14.2 органи місцевого самоврядування;

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

2.14.4 банки, інвестори, рейтингові агентства;

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

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

#### *3. Визначення вимог управління активами*

3.1. Інвентаризація активів: активи, пов’язані з інформацією та засобами обробки інформації, які зберігають, обробляють, передають інформацію, що підлягає захисту, мають бути ідентифіковані з документуванням цих активів за формою інвентаризаційного опису відповідно до D8.1-СУІБ «Положення щодо інвентаризації та обробки даних».

3.2. Виконком міської ради складає інвентаризаційний опис усіх своїх активів у межах сфери дії СУІБ та підтримує в актуальному стані інвентаризаційний опис активів СУІБ, включаючи апаратне забезпечення, програмне забезпечення, персонал, технології, інші ресурси для забезпечення функціонування СУІБ.

3.3. Процес складання інвентарного опису активів та ресурсів СУІБ є важливою передумовою управління ризиками.

3.4. Право власності на активи: для кожного ідентифікованого активу СУІБ погоджується та визначається власник активу, що має певну роль у СУІБ. Власник активу призначається рішенням виконкому міської ради із визначенням відповідальності за:

3.4.1 збереження активу;

3.4.2 використання активу виключно в межах області дії СУІБ;

3.4.3 дотримання відповідних вимог у галузі ІБ та кібербезпеки;

3.4.4 щоденний захист активу СУІБ.

3.5. Прийнятне використання активів: правила прийнятного використання активів і засобів обробки інформації визначені та задокументовані в D14.1-СУІБ «Політика ІТ-безпеки».

3.6. У сфері СУІБ наявні такі види доступу до активів:

3.6.1 стандартний доступ – доступ визначається як попередньо узгоджений набір доступів, властивих для посадових осіб виконкому міської ради;

3.6.2 нестандартний доступ – усі інші доступи, що не входять до стандартного доступу.

3.7. Доступ консультантів, розробників, аналітиків та інших спеціалістів до продуктивних систем або систем, що перебувають у дослідно-промисловій експлуатації, має бути обмеженим тільки на перегляд, окрім окремих випадків, пов’язаних з обслуговуванням систем або виправленням помилок, що заздалегідь погоджені із SOC.

3.8. Процес блокування доступу до активів:

3.8.1. Стандартне блокування доступу:

3.8.1.1 стандартне блокування доступу здійснюється в разі звільнення або переводу посадової особи на іншу посаду. Доступи не відключаються, якщо посадова особа переводиться на іншу посаду в рамках одного відділу, управління іншого виконавчого органу міської ради;

3.8.1.2 блокування доступу здійснюється на підставі заявки в системі Сервіс-Деск. Відповідальний за формування заявки в разі звільнення посадової особи – CHRO. Відповідальний за формування заявки в разі службової необхідності – керівник відділу, управління, іншого виконавчого органу міської ради, у штаті якого перебуває власник активу, якому потрібно скасувати доступ. Заявка може бути сформована як безпосередньо відповідальною посадовою особою, так і автоматично на основі даних про звільнення/переведення/тощо посадових осіб виконкому міської ради;

3.8.1.3 заявка маршрутизується до CIO та CISO. Заявка виконується згідно з процесом управління запитами.

3.8.2. Термінове блокування доступу:

3.8.2.1 термінове блокування доступу здійснюється при проведенні службових перевірок/розслідувань або при обробці інцидентів;

3.8.2.2 блокування доступу здійснюється на підставі заявки в системі Сервіс-Деск. У разі нагальної потреби запит щодо блокування доступу може бути наданий у телефонному або усному режимі. Проте це не відміняє створення заявки в системі Сервіс-Деск.

3.8.3 Відповідальний за формування заявки:

3.8.3.1 адміністратор безпеки за рішенням CSO або DPO (якщо це стосується обробки персональних даних) у разі проведення службових перевірок/розслідувань або обробки інциденту інформаційної безпеки;

3.8.3.2 адміністратор IRT у разі обробки ІТ інциденту;

3.8.3.3 заявка маршрутизується на адміністраторів відповідних підсистем і виконується згідно з процесом управління запитами.

3.8.4 Блокування доступу при відсутності активності.

3.8.4.1 якщо в ІКС відсутня активність облікового запису посадових осіб протягом 45 календарних днів, такий обліковий запис має бути відключений;

3.8.4.2 блокування доступу здійснюється на підставі заявки в системі Сервіс-Деск. Ініціаторами можуть виступати посадові особи SOC. До заявки прикріплюється список облікових записів, отриманий у результаті аудиту відповідної системи;

3.8.4.3 заявка на блокування доступу направляється до власника активу та відповідних адміністраторів підсистем для її виконання. Заявка виконується згідно з процесом управління запитами.

3.8.5 Видалення відключених облікових записів: для зменшення навантаження на ресурси ІКС та покращення управління обліковими записами, облікові записи архівуються та видаляються через 180 календарних днів з дати блокування доступу.

3.9. Процес розблокування доступу до активів визначений та задокументований у D14.1-СУІБ «Політика ІТ-безпеки», D14.14 «Політика контролю доступу».

3.10. Посадові особи та зацікавлені сторони, що пов’язані з активами в межах області дії СУІБ, повинні повернути всі активи виконкому міської ради, що перебувають у їх володінні, після припинення трудових відносин, контракту чи угоди.

3.11. Поводження з активами: посадові особи, які отримують активи в межах забезпечення процесів виконкому міської ради або обслуговують ці активи (щоденне технічне, регламентне, сезонне, гарантійне, післягарантійне обслуговування тощо), мають використовувати розумне судження та проявляти належну обережність, захищаючи й обслуговуючи активи СУІБ.

3.12. Посадові особи несуть відповідальність за організацію безпеки та належного догляду за обладнанням виконкому міської ради, коли воно транспортується чи зберігається за його межами. Утилізація та знищення активів проводиться відповідно до вимог D14.11-СУІБ «Політика утилізації та знищення».

3.13. З усіма мобільними пристроями слід поводитися відповідно до D14.3-СУІБ «Політика мобільних пристроїв, віддаленої роботи та роботи з дому» і D14.4-СУІБ «Політика щодо власного пристрою (BYOD)».

3.14. Усі особи, які виконують певну роль у СУІБ та мають доступ до інформації з обмеженим доступом, повинні підписати документ: «Заява про прийняття документів системи управління інформаційною безпекою» та дотримуватися правил, наведених у D4.1-СУІБ «Політики інформаційної безпеки», D4.6-СУІБ «Норми поведінки».

*\*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***