*ЗАТВЕРДЖЕНО*

 *Рішення виконкому міської ради*

*25.07.2025 №938*

***ПОЛІТИКА ЩОДО МОБІЛЬНИХ ПРИСТРОЇВ, ДИСТАНЦІЙНОЇ РОБОТИ ТА РОБОТИ З ДОМУ ВИКОНАВЧОГО КОМІТЕТУ***

***КРИВОРІЗЬКОЇ МІСЬКОЇ РАДИ***

#### *1. Загальні положення*

1.1. Політика щодо мобільних пристроїв, дистанційної роботи та роботи з дому виконавчого комітету Криворізької міської ради (надалі – Політика мобільних пристроїв) є документом для запобігання несанкціонованому доступу до мобільних пристроїв як у межах, так і за межами контрольованої зони (надалі – КЗ) виконкому міської ради в області дії системи управління інформаційною безпекою (надалі – СУІБ).

1.2. Політика мобільних пристроїв 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 EN ISO/IEC 27005:2023 (IDT; ISO/IEC 27005:2022, IDT) «Інформаційна безпека, кібербезпека та захист конфіденційності. Настанова керування ризиками інформаційної безпеки», ДСТУ ISO 31000:2018 (ISO 31000:2018, IDT) «Менеджмент ризиків. Принципи та настанови», ДСТУ ISO/IEC 27002:2023 (ISO/IEC 27002:2022, IDT) «Інформаційна безпека, кібербезпека та захист конфіденційності. Засоби контролювання інформаційної безпеки» (надалі – ISO 27002), 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 Re-vision 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», D2.2-СУІБ «Політика управління активами», D10-СУІБ «Методології оцінки та обробки ризиків», D14.6-СУІБ «Політика класифікації інформації», 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. 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 інформаційну безпеку (надалі – 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. Incident Response Team (надалі – IRT) – група реагування на інциденти.

2.9. 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.

2.10. 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.

2.11. 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 та систем.

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, між-народні 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, яка може вплинути на інформаційну безпеку та безперервність процесів. У контексті СУІБ Третя сторона може не мати створений та зареєстрований акаунт у межах області дії СУІБ. Це можуть бути сім’ї 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 інформаційну безпеку у межах області дії СУІБ.

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

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

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

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

#### *3. Мобільні пристрої*

3.1. Мобільні пристрої включають усі види портативних комп'ютерів, мобільних телефонів, смартфонів, карти пам'яті та іншого мобільного обладнання, призначеного для зберігання, обробки й передачі ІА у межах області дії СУІБ, незалежно від того чи це обладнання виконкому міської ради або перебуває у приватній власності (BYOD) користувача, що має певну роль у межах СУІБ та виконує функції в межах визначених повноважень за допомогою BYOD. Указане вище обладнання (BYOD) може бути використано за межами території виконкому міської ради лише після отримання дозволу від CEO за поданням CSO та виконання процедур стосовно:

3.1.1 попередження власника активу щодо обов’язковості дотримання процедур політик, процедур, правил СУІБ;

3.1.2 визначення персональної відповідальності за цей актив на час його перебування за межами контрольованої зони (надалі – КЗ) виконкому міської ради.

3.2. Посадова особа, яка користується мобільними пристроями за межами території виконкому міської ради, повинна дотримуватися таких правил:

3.2.1 мобільні пристрої, на яких зберігаються важливі, чутливі або критичні дані, не повинні залишатися без нагляду і, за можливості, їх слід фізично закривати або використовувати спеціальні замки для захисту обладнання;

3.2.2 при використанні мобільних пристроїв у громадських місцях користувач повинен ураховувати, щоб дані не могли бути прочитані несанкціонованими особами;

3.2.3 оновлення патчів та інших налаштувань системи здійснюються відповідно до «Політики керування виправленнями» (у межах виконання п. A.8.8 Додатка до ISO 27001);

3.2.4 захист від шкідливого коду встановлюється та оновлюється відповідно до політики захисту від шкідливих програм (у межах виконання п. A.8.7 Додатка до ISO 27001) (за можливості, використовуючи обов'язкове встановлення інструмента для захисту від зловживань та синхронізацію оновлень щонайменше раз на тиждень, використовуючи сервіси виконкому міської ради);

3.2.5 особа, яка використовує мобільні пристрої поза територією, відповідає за регулярне створення резервних копій даних, використовуючи мережу виконкому міської ради та виконуючи автоматичне/ручне резервне копіювання згідно з документом, який визначає резервне копіювання відповідно до D14.10-СУІБ «Політика резервного копіювання»;

3.2.6 підключення до комунікаційних мереж здійснюється за допомогою створення безпечного каналу зв'язку з використанням VPN із застосуванням технологій шифрування даних;

3.2.7 інформація на портативних комп'ютерах має бути зашифрована за допомогою шифрування файлів/папок. Обов’язковому шифруванню підлягають ІА, які відповідно до D14.6-CУІБ «Політика класифікації інформації» мають такі рівні конфіденційності:

3.2.7.1 «ЧУТЛИВА»;

3.2.7.2 «PII КОНФІДЕНЦІЙНО»;

3.2.7.3 «ДІЛОВА ІНФОРМАЦІЯ»;

3.2.7.4 «ТЕХНОЛОГІЧНА ІНФОРМАЦІЯ ЗАХИСТУ»;

3.2.8 захист ІА має бути реалізованим відповідно до D4.1-CУІБ «Політика інформаційної безпеки» з дотриманням правил захисту властивостей ІА щодо

відповідного рівня критичності згідно з D14.6-CУІБ «Політика класифікації інформації»;

3.2.9 власник активу, який використовує мобільні пристрої поза КЗ виконкому міської ради, зобов’язаний дотримуватися інструкцій виробника щодо захисту обладнання (наприклад, забезпечити захист від погодних умов, впливу електромагнітних перешкод, фізичних вібрацій тощо);

3.2.10 коли користувачі ЄІС використовують власні пристрої, слід застосовувати правила, визначені D14.4-СУІБ «Політика використання власного пристрою (BYOD)».

3.3. CSO разом з CHRO відповідають за навчання та підвищення обізнаності користувачів ЄІС, власників активів, що використовують мобільні пристрої поза межами виконкому міської ради.

#### *4. Віддалена робота та робота з дому*

4.1. Віддалена робота означає, що інформаційно-комунікаційне обладнання використовується для забезпечення інформаційної діяльності посадових осіб поза КЗ виконкому міської ради, включаючи роботу з дому. Віддалена робота не передбачає використання мобільних телефонів за межами території виконкому міської ради.

4.2. Віддалена робота має бути санкціонована дозволом CEO за допомогою таких способів:

4.2.1 дозвіл може бути наданий усно (якщо цей користувач ЄІС буде працювати з інформацією, що класифікована як «ПУБЛІЧНА» та «ДЛЯ ВНУТРІШНЬОГО ВИКОРИСТАННЯ»);

4.2.2 у письмовій формі шляхом надсилання електронною поштою або підписання документа власноручно чи із використанням технології кваліфікованого електронного підпису («Docusign») (якщо цей користувач ЄІС буде працювати з інформацією «ЧУТЛИВА»; «PII КОНФІДЕНЦІЙНО»; «ДІЛОВА ІНФОРМАЦІЯ» та «ТЕХНОЛОГІЧНА ІНФОРМАЦІЯ ЗАХИСТУ») з дотриманням вимог політики доступу в межах правил розмежування доступу та дотриманням вимог щодо шифрування ІА під час їх зберігання на робочій станції користувача ЄІС та передачі через незахищене середовище відповідно до вимог D14.12-СУІБ «Політика використання шифрування».

4.3. Усі користувачі ЄІС, які здійснюють віддалену роботу, повинні дотримуватися захисту мобільних пристроїв, а також таких правил проведення дистанційної роботи:

4.3.1 запобігання несанкціонованому доступу сторонніх осіб (зацікавлених сторін та третіх осіб) за допомогою використання кабінетів і приміщень з можливістю зачиняти двері, відсутність роботи в громадських місцях, розташування, що не допускає можливості іншим бачити або чути інформацію тощо;

4.3.2 уникнення від зовнішніх загроз, таких як: крадіжки, пожежі тощо за допомогою використання охоронців, відеоспостереження, сигналізаційних систем, вогнестійких стін тощо;

4.3.3 захист пристроїв у роботі та на зберіганні за допомогою шаф і столів з замками, сейфів тощо;

4.3.4 видалення ідентифікаційних знаків (паролів та інших нотаток, які розкривають ІА, технологічну інформацію захисту, що може привести до витоку інформації з обмеженим доступом та порушенню вимог СУІБ) на відкритих майданчиках (стіна, стіл, папірець тощо);

4.3.5 наявність у посадових осіб, які виконують віддалену роботу, безперебійного джерела живлення, альтернативних комунікаційних ланок (якщо можливо підключитися до мережі «Інтернет» через постачальника інтернет-послуг, який має сертифікат безпеки ISO 27001 або Атестат відповідності комплексної системи захисту інформації, який підтверджує відповідність захищеного вузла інтернет-доступу до вимог чинного законодавства у системі технічного захисту інформації в Україні);

4.3.6 захист прав інтелектуальної власності виконкому міської ради як для програмного забезпечення, так і для інших матеріалів, які можуть бути захищені правами інтелектуальної власності відповідно до «Політики класифікації інформації».

4.4. Конкретні дії для посадових осіб, які здійснюють віддалену роботу, передбачають заборону:

4.4.1 передачі свого пристрою кому-небудь без шифрування всієї інформації з рівнем конфіденційності «ЧУТЛИВА», ««PII КОНФІДЕНЦІЙНО»; «ДІЛОВА ІНФОРМАЦІЯ» та «ТЕХНОЛОГІЧНА ІНФОРМАЦІЯ ЗАХИСТУ»;

4.4.2 надсилання інформації з обмеженим доступом («ЧУТЛИВА», ««PII КОНФІДЕНЦІЙНО»; «ДІЛОВА ІНФОРМАЦІЯ» та «ТЕХНОЛОГІЧНА ІНФОРМАЦІЯ ЗАХИСТУ») у відкритому вигляді без застосування технології шифрування;

4.4.3 самостійної зміни конфігурацій на мобільних пристроях;

4.4.4 участі в закритих зустрічах з включеною відеокамерою;

4.4.5 відсутності зв'язку під час робочих годин при дзвінку тривалістю понад 30 хвилин;

4.4.6 використання робочих мобільних пристроїв для власних потреб поза робочими годинами.

4.5. Конкретні дії, дозволені при виконанні дистанційної роботи, включають використання BYOD для власних потреб поза робочими годинами з дотриманням вимог політик СУІБ.

#### *5. Політика віддаленого доступу*

5.1. CSO готує та погоджує у CEO перелік осіб, які мають право на виконання завдань у режимі віддаленого доступу. CISO має контролювати дотримання заходів безпеки для захисту інформації та інших активів СУІБ під час роботи посадових осіб віддалено. CIO забезпечує доступ повноважних осіб до сервісів ЄІС з дотриманням вимог політик СУІБ з максимальним обмеженням прав користувачів, які виконують віддалений доступ.

5.2. Перед тим як ухвалити рішення щодо того, хто може отримати віддалений доступ, CSO враховує:

5.2.1 існуючий чи запропонований фізичний захист робочого місця на віддаленій локації, ураховуючи фізичну безпеку місця і місцеве середовище, включаючи різні юрисдикції, де перебувають посадові особи;

5.2.2 правила та механізми безпеки для фізичного середовища на віддаленій локації, такі як: зачинені шафи для зберігання документів, безпечний транспорт між локаціями, правила для віддаленого доступу, чистого робочого столу, друку та утилізації інформації та інших пов'язаних активів, а також повідомлення про події з ІБ;

5.2.3 очікувані фізичні умови дистанційної роботи;

5.2.4 вимоги щодо безпеки зв'язку, ураховуючи потребу віддаленого доступу до ЄІС, чутливість інформації, яку слід отримувати та передавати по комунікаційному каналу, а також чутливість систем і додатків;

5.2.5 використання віддаленого доступу, такого як доступ до віртуального робочого столу, який підтримує обробку та зберігання інформації на особистому обладнанні;

5.2.6 загрозу несанкціонованого доступу до інформації чи ресурсів інших осіб на віддаленому робочому місці (наприклад, родичів та друзів);

5.2.7 загрозу несанкціонованого доступу до інформації чи ресурсів інших осіб у громадських місцях;

5.2.8 використання домашніх і громадських мереж та вимоги чи обмеження щодо конфігурації бездротових мережевих служб;

5.2.9 використання засобів безпеки, таких як: брандмауери (програма чи пристрій, що здійснює захист комп'ютерних мереж) та захист від шкідливого програмного забезпечення;

5.2.10 безпечні механізми для розгортання та ініціалізації систем віддалено;

5.2.11 безпечні механізми для аутентифікації та активації привілеїв доступу, ураховуючи вразливість механізмів однофакторної аутентифікації у випадку дозволу віддаленого доступу до ЄІС.

5.3. Виконком міської ради впроваджує технічні та організаційні заходи для забезпечення захисту PII відповідно до рівня конфіденційності PII (за умови попереднього дозволу від CEO відповідному користувачу працювати з PII), зокрема:

5.3.1 псевдонімізацію та шифрування РІІ;

5.3.2 можливість забезпечення постійної конфіденційності, цілісності, доступності PII та стійкості ЄІС;

5.3.3 можливість повноважним особам доступу до РІІ або відновлення доступності PII у найкоротший строк у разі фізичного чи технічного інциденту;

5.3.4 процес для регулярного тестування, оцінювання та оцінки ефективності технічних і організаційних заходів для організації безпеки обробки.

5.4. При оцінці відповідного рівня безпеки слід, зокрема ураховувати ризики, що виникають внаслідок обробки, зокрема випадкового чи неправомірного

знищення, втрати, зміни, несанкціонованого розкриття або доступу до PII, переданих, збережених чи оброблених іншим чином.

5.5. Дотримання затвердженого кодексу поведінки (більш детально наведено в D4.6-СУІБ «Кодекс поведінки»), як зазначено у статті 40 GDPR, чи затвердженого механізму сертифікації, як зазначено у статті 42 GDPR, може використовуватися як елемент, що демонструє відповідність виконкому міської ради вимогам ISO 27001, ISO 27701.

5.6. DPO здійснює контроль, щоб суб’єкт PII, дані якого оброблюються засобами контролера PII або процесора PII у межах області дії СУІБ, мав доступ до власних PII. При цьому інші особи, навіть ті які мають або не мають певної ролі в межах області дії СУІБ (працівники контролера PII, процесора PII, постачальників послуг, інші суб’єкти PII), не мали права їх обробляти, поки суб’єкт PII не надасть згоду на таку обробку в межах конкретних цілей. Виключенням із цього правила може бути коли випадок розкриття PII вимагається чинним законодавством, що регулює процес захисту та обробки PII.

5.7. Належні рекомендації та заходи контролю безпеки включають:

5.7.1 надання відповідного обладнання для здійснення дистанційної роботи;

5.7.2 використання мобільного обладнання;

5.7.3 визначення дозволеної роботи, класифікації інформації, яку можна утримувати, та внутрішніх систем і послуг, доступ до яких має уповноважена посадова особа для віддаленої роботи;

5.7.4 забезпечення навчання для тих, хто працює віддалено, та тих, хто надає підтримку. Це включає методи проведення навчання в безпечний спосіб під час дистанційної роботи;

5.7.5 надання відповідного комунікаційного обладнання, включаючи методи забезпечення віддаленого доступу, такі як:

5.7.5.1 VPN;

5.7.5.2 політики безпеки (вимоги до блокування екрану пристрою та таймерів бездіяльності);

5.7.5.3 доступ без довіри (Zero-Trust Access – це сучасне рішення для всіх проблем. Воно виходить з концепції «ніколи не довіряй, завжди перевіряй». Сервіс вважає, що мережа вже перебуває під загрозою; отже, він перевіряє кожного користувача/пристрій перед прийняттям будь-яких рішень);

5.7.5.4 системи запобігання та виявлення вторгнень (допомагають захищати застосунки та мережі й пом'якшують атаки);

5.7.5.5 брандмауер;

5.7.5.6 менеджер паролів та багатофакторна аутентифікація;

5.7.5.7 шифрування та резервне копіювання даних;

5.7.5.8 навчання посадових осіб виконкому міської ради;

5.7.5.9 управління ідентичністю та доступом (для керування користувачами, паролями та рівнями доступу).

5.7.6 включення слідкування за місцем розташування пристрою;

5.7.7 установлення можливостей віддаленого видалення даних;

5.7.8 фізична безпека;

5.7.9 правила й поради щодо доступу сім'ї і відвідувачів до обладнання та інформації;

5.7.10 надання підтримки й обслуговування обладнання та програмного забезпечення;

5.7.11 надання страхування;

5.7.12 процедури резервного копіювання та продовження інформаційної діяльності;

5.7.13 аудит та моніторинг безпеки;

5.7.14 скасування повноважень і прав доступу та повернення обладнання при припиненні віддалених робочих дій.

\**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***