*ЗАТВЕРДЖЕНО*

 *Рішення виконкому міської ради*

*25.07.2025 №938*

***ПОЛІТИКА ВЛАСНОГО ПРИСТРОЮ (BYOD)***

***ВИКОНАВЧОГО КОМІТЕТУ КРИВОРІЗЬКОЇ МІСЬКОЇ РАДИ***

#### *1. Загальні положення*

1.1. Політика власного пристрою (Bring your own device) виконавчого комітету Криворізької міської ради (надалі – BYOD) є документом для визначення чітких правил обліку та прийнятного використання власних пристроїв, що використовують користувачі для доступу до сервісів Єдиної інформаційної системи міста Кривий Ріг (надалі – ЄІС) у межах області дії системи управління інформаційної безпеки (надалі – СУІБ).

1.2. BYOD застосовується до всіх власних пристроїв у межах області дії СУІБ в незалежності від того, використовуються вони в особистих або службових цілях та чи використовуються вони в приміщеннях виконкому міської ради або за його межами.

1.3. BYOD застосовується до всього обсягу СУІБ та конфіденційністю, а саме: усіх інформаційних систем/підсистем та інших інформаційних активів, що використовуються в межах СУІБ, а також всіх дій з обробки персональних даних.

1.4. BYOD 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 27005:2023 (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», 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», D2.2-СУІБ «Політика управління активами»; D10-СУІБ «Методології оцінки та обробки ризиків», D14.3-СУІБ «Політика щодо мобільних пристроїв, дистанційної роботи та роботи з дому», 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, що 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 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. Bring your own device (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.

2.11. PII – персональні дані.

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

2.13. Ad1 – адміністратор безпеки.

2.14. Ad2 – адміністратор системи.

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

2.16. [Брандмауер](https://uk.wikipedia.org/wiki/%D0%9C%D0%B5%D1%80%D0%B5%D0%B6%D0%B5%D0%B2%D0%B8%D0%B9_%D0%B5%D0%BA%D1%80%D0%B0%D0%BD) — програма чи пристрій, що здійснює захист комп'ютерних мереж.

#### *3.* *Використання особистих пристроїв*

3.1. Використання BYOD в робочих цілях дозволяється тільки обмеженому колу осіб і тільки за умови виконання вимог, що пред'являються до таких пристроїв. Будь-яка інформація, що зберігається, обробляється чи передається BYOD є власністю виконкому міської ради, який залишає за собою право контролювати таку інформацію.

3.2. На користувачів BYOD розповсюджується дія всіх документів СУІБ, що встановлюють порядок комплектування та налаштування програмного забезпечення (надалі – ПЗ), підключення до ЄІС, повернення встановленого ПЗ та інформаційних ресурсів, які виготовлені на користь виконкому міської ради в процесі виконання посадових обов’язків. У разі отримання дозволу використання BYOD слід ураховувати таке:

3.2.1 розподіл на особисте користування пристроями та в межах посадових обов’язків, включаючи використання ПЗ для їх підтримки, а також відокремлення та захист даних на приватному пристрої;

3.2.2 надання доступу до інформації, у тому числі PII, лише після того, як користувачі визнають свої обов’язки (фізичний захист, оновлення програмного забезпечення, уключаючи інсталяцію та налаштування комплексу криптографічного захисту інформації і комплексу засобів захисту), відмова від права власності на дані, що дозволяє видалення даних повноважними особами виконкому міської ради, а саме: CSO, DPO, CISO, Ad1 у разі крадіжки чи втрати пристрою або коли вони більше не мають права на використання сервісів ЄІС. Якщо відбулася втрата PII, у таких випадках слід ураховувати законодавство про захист PII;

3.2.3 тематичні політики та процедури для запобігання спорам щодо прав на інтелектуальну власність, розроблених на приватному обладнанні;

3.2.4 доступ до приватного обладнання (для перевірки безпеки або під час розслідування), яким можна запобігти порушенню законодавства користувачем BYOD;

3.2.5 ліцензійні угоди на програмне забезпечення, за які виконком міської ради може взяти на себе відповідальність за ліцензування клієнтського програмного забезпечення на кінцевих пристроях користувача BYOD, що належать посадовим особам або стороннім користувачам.

#### *4. Користувачі та цілі використання BYOD*

4.1. CSO створює і підтримує список посад та/або осіб разом з переліком прикладного ПЗ і баз даних, до яких дозволений доступ з використанням BYOD. CIO, Ad2, відповідальний за програмне забезпечення створюють і підтримують список програм і баз даних, для яких надано доступ з використанням BYOD.

4.2. CISO під керівництвом CSO виконує завдання з налаштування правил розмежування доступу за принципом надання мінімальних повноважень користувачам BYOD. CISO створює і підтримує список пристроїв BYOD, які можуть використовуватися для виконання користувачами посадових обов'язків, та перелік додаткових обов'язкових вимог до кожного такого пристрою.

#### *5. Прийнятне використання політики власного пристрою*

5.1. Правила застосування BYOD:

5.1.1 регулярне створення резервних копій ІА на мережеві диски зберігання виконкому міської ради;

5.1.2 наявність антивірусного програмного забезпечення і автоматичного завантаження оновлень;

5.1.3 наявність оновлень безпеки й автоматичне завантаження нових оновлень;

5.1.4 наявність брандмауера з попередньо встановленими правилами;

5.1.5 наявність засобів шифрування для забезпечення захисту інформації відповідно до вимог СУІБ;

5.1.6 наявність засобів створення VPN-підключень до ізольованої мережі ЄІС;

5.1.7 при використанні власних пристроїв за межами контрольованої зони виконкому міської ради, такі пристрої не повинні залишатися без нагляду;

5.1.8 при використанні власних пристроїв у громадських місцях, власник уживає заходів, щоб дані не могли бути прочитані сторонніми особами;

5.1.9 перед утилізацією, продажем або передачею власного пристрою третім особам для обслуговування слід повідомити CSO.

5.2. Заборонені дії при застосуванні BYOD:

5.2.1 надавати стороннім особам доступ до власного пристрою;

5.2.2 установлювати додатки, заборонені до використання на власних пристроях;

5.2.3 зберігати й установлювати неліцензійне програмне забезпечення;

5.2.4 зберігати матеріали, що можуть бути визнані об'єктами авторського права;

5.2.5 підключатися через технологію «Bluetooth» до інших пристроїв;

5.2.6 підключатися до невідомих мереж «Wi-Fi»;

5.2.7 передавати дані виконкому міської ради на недозволені пристрої та мережі.

#### *6. Особливі повноваження*

6.1. Повноважні особи виконкому міської ради мають право переглядати, редагувати й видаляти всі дані виконкому міської ради, що зберігаються, передаються або обробляються на власних пристроях.

6.2. CISO/Ad1/Ad2 за командою CSO уповноважений конфігурувати будь-який власний пристрій відповідно до вимог BYOD та контролювати його використання засобами віддаленого моніторингу й доступу.

6.3. Повноважні особи мають право здійснювати повне видалення всіх даних на власному пристрої без згоди власника пристрою, якщо це буде потрібно для захисту даних у межах цілей інформаційної діяльності виконкому міської ради.

6.4. Виконком міської ради встановлює процедури для:

6.4.1 налаштування бездротових з’єднань на пристроях (наприклад, відключення вразливих протоколів);

6.4.2 використання бездротових або дротових з’єднань з відповідною пропускною здатністю згідно з відповідними вимогами політик СУІБ (наприклад тому, що потрібні резервні копії або оновлення програмного забезпечення).

#### *7. Порушення безпеки*

7.1. Усі порушення безпеки, пов'язані з використанням компонентів ЄІС або з власним пристроєм, користувачі ЄІС повинні негайно довести до відома CISO. Більше того, усі недоліки безпеки, що можуть стати причиною виникнення інциденту мають бути доведені до відома CSO користувачами ЄІС протягом одного робочого дня, після того, як стало про них відомо або є передумова їх неминучої появи.

7.2. Для надання можливості BYOD працювати в ЄІС, необхідно провести оцінку ризиків з розглядом таких відомостей:

7.2.1 елементи керування для захисту інформації на кінцевих пристроях користувача залежать від того, чи пристрій кінцевої точки користувача використовується лише всередині захищених приміщень виконкому міської ради та мережевих з’єднань, чи за межами організації, що призводить до збільшення фізичних і мережевих загроз;

7.2.2 бездротові підключення для кінцевих пристроїв користувача подібні до інших типів мережевих підключень, але мають важливі відмінності, які слід ураховувати при визначенні засобів контролю. Зокрема резервне копіювання інформації, що зберігається на кінцевих пристроях користувача, іноді може не працювати через обмежену мережеву пропускну здатність або через те, що кінцеві пристрої користувача не підключені в той час, коли заплановано проведення резервного копіювання;

7.2.3 для деяких портів USB, наприклад USB-C, вимкнути порт USB неможливо, оскільки він використовується для інших цілій (наприклад, подача живлення та вихід на дисплей).

#### *8. Навчання та підвищення обізнаності*

CSO сумісно з CHRO є відповідальними за підготовку планів навчання та підвищення обізнаності всіх посадових осіб виконкому міської ради щодо правильного використання власних пристроїв і протидії найбільш істотним загрозам, пов'язаних з використанням BYOD.

*\*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***