Додаток №5 до Протоколу №12 засідання
Молодіжної ради при Миколаївській міській раді
від 26 вересня 2025 року

Політика інформаційної безпеки
Молодіжної ради при Миколаївській міській раді

1. Загальні положення

Молодіжна рада при Миколаївській міській раді (далі — Рада) визнає важливість забезпечення конфіденційності, цілісності та доступності інформації, що створюється, використовується або зберігається у процесі діяльності Ради.

Ця Політика встановлює правила і принципи інформаційної безпеки, спрямовані на захист даних, у тому числі персональних, а також цифрових ресурсів Ради від несанкціонованого доступу, зловживань, втрати чи пошкодження.

2. Мета

— захистити інформаційні ресурси Ради від внутрішніх і зовнішніх загроз;
— забезпечити належне поводження з персональними та конфіденційними даними;
— гарантувати безпечне використання інформаційно-комунікаційних технологій;
— зберегти довіру партнерів, учасників, бенефіціарів та громади.

3. Сфера дії

Ця політика поширюється на:
— членів Ради;
— працівників, волонтерів, консультантів, експертів, партнерів;
— будь-які пристрої, системи, сервіси, акаунти та бази даних, що використовуються Радою.

4. Основні принципи

— Конфіденційність. Інформація обробляється так, щоб доступ до неї мали лише уповноважені особи.
— Цілісність. Дані захищені від спотворення, несанкціонованих змін або знищення.
— Доступність. Інформація доступна для законного використання тоді, коли вона потрібна.
— Законність. Уся обробка інформації здійснюється відповідно до законодавства України та міжнародних норм.
— Мінімізація даних. Збираються лише ті дані, що необхідні для реалізації завдань Ради.
— Прозорість. Учасники поінформовані про те, як використовуються їхні дані.

5. Категорії інформації

1. Публічна інформація — дані, що підлягають відкритому доступу (оголошення, новини, звіти).

2. Внутрішня інформація — службова кореспонденція, внутрішні документи.

3. Конфіденційна інформація — персональні дані, фінансові відомості, чутливі проєктні матеріали.

6. Захист персональних даних

— Персональні дані обробляються виключно за згодою суб'єкта або на законних підставах.
— Дані зберігаються у захищених базах із доступом лише для уповноважених осіб.
— У разі витоку чи зламу Рада зобов'язана повідомити постраждалих та вжити заходів для мінімізації ризиків.

7. Організаційні заходи

— призначення відповідальної особи з питань інформаційної безпеки;
— проведення навчань для членів Ради з питань безпечної роботи з даними;
— створення внутрішніх інструкцій для роботи з інформацією та комунікаційними платформами;
— укладення угод про нерозголошення (NDA) з партнерами та консультантами у разі доступу до конфіденційної інформації.

8. Технічні заходи

— використання надійних паролів і двофакторної автентифікації;
— регулярне оновлення програмного забезпечення;
— резервне копіювання важливих даних;
— обмеження доступу до спільних ресурсів лише для уповноважених осіб;
— використання офіційних і захищених комунікаційних каналів.

9. Процедури реагування на інциденти

— У разі виявлення загрози (злам акаунта, витік даних, підозріла активність) відповідальна особа негайно інформує керівництво Ради.
— Здійснюється фіксація інциденту та аналіз причин.
— Вживаються заходи для усунення наслідків (зміна паролів, відновлення даних із резервних копій).
— У разі порушення законодавства інформуються відповідні органи.

10. Відповідальність

— Члени Ради зобов'язані дотримуватися цієї політики.
— Порушення правил інформаційної безпеки тягне за собою дисциплінарну відповідальність (аж до виключення зі складу Ради) та може стати підставою для юридичної відповідальності згідно із законодавством.

11. Моніторинг та перегляд

— Політика переглядається щороку або у разі змін у законодавстві чи міжнародних стандартах.
— Рада впроваджує внутрішній моніторинг дотримання правил інформаційної безпеки.

Голова Молодіжної ради при Миколаївській міській раді **Герило А. М.**

Секретар Молодіжної ради при Миколаївській міській раді **Мартинишин Н. А.**