



ПОЛІТИКА УПРАВЛІННЯ РИЗИКАМИ

RISK MANAGEMENT POLICY

Організація	МГЕО «Наш Дім - Манява»
Версія	2.2 FINAL
Попередня версія	2.1 / 2.0
Дата затвердження	13.06.2026
Дата перегляду	Щорічно або раніше у разі змін безпекового контексту, донорських вимог, законодавства, програмної діяльності чи внутрішніх процедур
Відповідальний	Керівник Організації / відповідальна особа з управління ризиками та безпеки
Пов'язані політики	Політика захисту дітей і вразливих груп; Кодекс етики та поведінки; Політика конфіденційності та захисту персональних даних; Антикорупційна політика; Політика екологічної, кліматичної та громадської відповідальності; Політика фінансового управління та закупівель; Політика моніторингу, оцінки, підзвітності та навчання; Політика цифрового врядування та етики штучного інтелекту
Сайт	https://ourhomemanyava.com

Примітка до версії

Ця версія v2.2 оновлює Політику управління ризиками v2.1 та посилює її відповідність новій інституційній архітектурі МГЕО «Наш Дім - Манява». Документ інтегрує ризики Карпатської ініціативи екологічної стійкості та сталості на 2026-2028 роки, зокрема ризики для дітей і вразливих груп, польових активностей, малих річок, відкритих екологічних даних, цифрових інструментів, фінансів, закупівель, репутації, донорської відповідності, воєнного контексту та безперервності діяльності.

У v2.2 додано блоки щодо добробуту команди й волонтерів, страхування, кризових комунікацій, теплової карти ризиків, посиленого плану безперервності діяльності та узгодження оцінки партнерів із фінансовою політикою Організації.

Українська версія цієї Політики є основною робочою версією Організації. Коротке резюме англійською мовою надається для донорів і міжнародних партнерів.

Зміст

1. Мета та сфера застосування
2. Основні принципи управління ризиками
3. Зв'язок із Карпатською ініціативою 2026-2028
4. Процес управління ризиками
5. Категорії ризиків
6. Оцінка рівня ризику
7. Ризики для дітей, молоді та вразливих груп
8. Екологічні, кліматичні та польові ризики
9. Воєнні та безпекові ризики
10. Цифрові ризики, дані, геодані та штучний інтелект
11. Фінансові, закупівельні та антикорупційні ризики
12. Репутаційні ризики та екологічні маніпуляції
13. Операційні, кадрові ризики та добробут команди
14. Страхування, безпека учасників і захист активів
15. Ризики партнерств, субгрантів і підрядників
16. Реєстр ризиків
17. Реагування на інциденти та ескалація
18. Кризові комунікації під час серйозних інцидентів
19. Безперервність діяльності
20. Зв'язок із моніторингом, оцінкою, підзвітністю та навчанням
21. Ролі та відповідальність
22. Перегляд політики
23. Додатки
24. Коротке резюме англійською мовою

Українська версія

1. Мета та сфера застосування

Ця Політика визначає принципи, правила та мінімальні процедури управління ризиками в діяльності МГЕО «Наш Дім - Манява».

Метою Політики є своєчасне виявлення, оцінка, зменшення, моніторинг і документування ризиків, які можуть впливати на дітей, молодь і вразливі групи; громади, школи, партнерів і учасників заходів; команду, волонтерів, консультантів і підрядників; природні екосистеми, малі річки, водні об'єкти, ліси, ґрунти та природоохоронні території; персональні дані, фото, відео, геодані та цифрові системи; фінансові ресурси, закупівлі, активи та донорські кошти; репутацію, довіру та публічну комунікацію Організації; безперервність діяльності в умовах війни, криз, перебоїв зв'язку, електропостачання або інших надзвичайних ситуацій.

Політика застосовується до всіх програм, проєктів, заходів, партнерств, польових активностей, освітніх сесій, досліджень, закупівель, субгрантів, цифрових інструментів, публікацій і донорської звітності Організації.

2. Основні принципи управління ризиками

- Попередження ризиків: краще запобігати ризику на етапі планування, ніж реагувати після інциденту.
- Принцип «не нашкодь»: діяльність не повинна створювати неприйнятної шкоди людям, дітям, громадам, довкіллю, водним ресурсам, даним, репутації або довірі.
- Недопущення значної шкоди: екологічні, соціальні та безпекові ризики мають оцінюватися до початку активності.
- Пропорційність: рівень аналізу ризику має відповідати масштабу, складності й потенційному впливу активності.
- Доказовість: рішення щодо ризиків мають документуватися та спиратися на факти, консультації, чеклисти, оцінки або професійне судження.
- Захист дітей і вразливих груп: ризики для дітей, молоді, ВПО, людей з інвалідністю, дітей військовослужбовців, малозабезпечених родин та інших груп оцінюються з підвищеною обережністю.
- Обов'язок турботи: Організація враховує фізичну, психологічну та цифрову безпеку команди, волонтерів і учасників.
- Підзвітність: громади, учасники, партнери й донори мають мати зрозумілі канали для повідомлення про ризики, інциденти або скарги.
- Навчання: кожен суттєвий ризик, інцидент або помилка мають використовуватися для покращення процедур.

3. Зв'язок із Карпатською ініціативою 2026-2028

Ця Політика є частиною інституційної рамки Карпатської ініціативи екологічної стійкості та сталості МГЕО «Наш Дім - Манява» на 2026-2028 роки.

Кожен новий проєкт або значна активність у межах Карпатської ініціативи має проходити базову оцінку ризиків до початку реалізації.

- екологічна освіта дітей і молоді;
- малі річки, вода, санітарія, гігієна та водна безпека;
- зелена лабораторія і практичне навчання;
- екобібліотека та мультимедійний екоцентр;
- відкриті екологічні дані;
- зелені простори гідності дітей;
- природоорієнтовані рішення;
- польові активності в природі;
- партнерства з громадами, школами, природоохоронними установами та органами місцевого самоврядування;
- донорські проєкти, фінанси, закупівлі та субгранти.

4. Процес управління ризиками

Організація застосовує простий цикл управління ризиками: виявлення, аналіз, оцінка, рішення щодо реагування, документування, моніторинг і навчання.

- Виявлення ризику - визначити, що може піти не так і кого або що це може зачепити.
- Аналіз ризику - оцінити ймовірність і можливий вплив.
- Оцінка рівня ризику - визначити, чи є ризик низьким, середнім, високим або критичним.
- Рішення щодо реагування - уникнути, зменшити, передати, прийняти або зупинити активність.
- Документування - зафіксувати ризик, рішення, відповідальну особу і строки.
- Моніторинг - перевіряти, чи ризик зменшився або змінився.
- Навчання - використати досвід для покращення наступних активностей.

5. Категорії ризиків

- ризики для дітей, молоді та вразливих груп;
- екологічні та кліматичні ризики;
- польові ризики та ризики заходів у природі;
- воєнні та безпекові ризики;
- цифрові ризики, ризики даних і геоданих;
- фінансові та закупівельні ризики;
- антикорупційні ризики;
- репутаційні ризики;
- операційні, кадрові та психологічні ризики;
- ризики партнерств, підрядників і субгрантів;
- донорські та юридичні ризики;
- ризики безперервності діяльності.

6. Оцінка рівня ризику

Організація оцінює ризики за двома критеріями: ймовірність і вплив. Якщо ризик стосується життя, здоров'я, дітей, сексуальної експлуатації чи насильства, воєнної безпеки, значної шкоди довкіллю, шахрайства або серйозного порушення закону, він автоматично розглядається як високий або критичний.

Рівень ризику	Опис	Дія
Низький	Ризик малоімовірний або має незначний вплив	Активність може проводитися зі звичайним контролем
Середній	Ризик можливий або має помірний вплив	Потрібні додаткові запобіжні заходи
Високий	Ризик імовірний або може мати серйозні наслідки	Потрібне погодження керівника, план зменшення ризику і документування
Критичний	Ризик може спричинити серйозну шкоду людям, дітям, безпеці, довкіллю, фінансам або репутації	Активність зупиняється, переноситься або не реалізується без належного рішення та заходів безпеки

7. Ризики для дітей, молоді та вразливих груп

Організація визнає, що діяльність із дітьми, молоддю та вразливими групами потребує підвищеної обережності.

- фізична небезпека під час заходів, поїздок або польових активностей;
- психологічний дискомфорт, тиск або стигматизація;
- неналежна поведінка дорослих щодо дітей;
- фото, відео або історії без належної згоди;
- збір зайвих персональних даних;
- недоступність заходів для дітей з інвалідністю або інших груп;
- відсутність супроводу, укриття, першої допомоги або плану безпеки.
- Мінімальні заходи: застосування Політики захисту дітей і вразливих груп; згода батьків або законних представників; інструктаж команди; присутність відповідальних дорослих; безпечне місце; доступний механізм звернень і скарг.

8. Екологічні, кліматичні та польові ризики

Екологічні й польові ризики можуть виникати під час заходів у природі, біля річок, джерел, лісів, природоохоронних територій, шкільних зелених просторів або громадських локацій.

- пошкодження рослинності, берегів, ґрунтів або оселищ;
- забруднення або засмічення території;
- порушення спокою тварин;
- небезпечні погодні умови, паводки, зсуви, ожеледиця, спека або сильні опади;
- відсутність доступу до води, санітарії, укриття або зв'язку;
- помилкова інтерпретація освітніх водних тестів;
- публікація чутливих геоданих природних об'єктів.
- Мінімальні заходи: базовий екологічний і соціальний скринінг; чеклист польової активності; перевірка погоди та маршруту; інструктаж учасників; правило «не залишати слідів»; обережна комунікація про водні тести.

9. Воєнні та безпекові ризики

Організація працює в умовах повномасштабної війни в Україні, тому безпекові ризики мають пріоритет.

- повітряна тривога під час заходу;
- ракетна або дронна атака;
- відсутність укриття;
- перебої електроенергії, зв'язку або інтернету;
- обмеження пересування;
- психологічна втома учасників і команди;
- ризики публікації точних маршрутів, координат або фото;
- ризики для критичної інфраструктури або природоохоронних об'єктів.
- Мінімальні заходи: захід не проводиться без розумного плану безпеки; під час повітряної тривоги активність зупиняється; учасники переходять до укриття або безпечного місця; польові виїзди не проводяться під час безпекового загострення.

10. Цифрові ризики, дані, геодані та штучний інтелект

Цифрові ризики пов'язані з використанням електронної пошти, хмарних сховищ, KoboToolbox, геоінформаційних систем, онлайн-форм, сайту, соціальних мереж, штучного інтелекту, фото, відео та цифрових мап.

- втрата доступу до акаунтів або витік персональних даних;
- збір зайвих даних або публікація чутливих геоданих;
- фішинг або шахрайські листи;
- використання штучного інтелекту для створення неперевірених або вигаданих даних;
- неправильна інтерпретація цифрових карт або дашбордів;
- втрата даних через технічний збій.
- Мінімальні заходи: доступ лише для уповноважених осіб; двофакторна автентифікація там, де доступна; резервне копіювання; очищення даних перед публікацією; заборона вигаданих даних, цитат, результатів або доказів.

11. Фінансові, закупівельні та антикорупційні ризики

- нецільове використання коштів або відсутність підтвердних документів;
- порушення закупівельної процедури;
- конфлікт інтересів або змова постачальників;
- завищення вартості;
- неналежна перевірка постачальників;
- санкційні або репутаційні ризики;
- помилки в авансах, валютах або звітності;
- невірний облік власного або негрошового внеску.

- Мінімальні заходи: дотримання Політики фінансового управління та закупівель; дотримання Антикорупційної політики; перевірка постачальників у ризикових випадках; документування закупівель; внутрішній контроль; зберігання документів.

12. Репутаційні ризики та екологічні маніпуляції

- звинувачення без доказів;
- представлення освітніх водних тестів як офіційних висновків;
- перебільшення результатів;
- використання фото дітей або вразливих груп без належної згоди;
- публікація чутливих даних;
- некоректна критика громади, установи або партнера;
- екологічні маніпуляції або політизована комунікація.
- Мінімальні заходи: перевірка фактів перед публікацією; розмежування фактів, припущень і попередніх спостережень; обережна мова; погодження чутливих публікацій; пояснення обмежень громадської науки.

13. Операційні, кадрові ризики та добробут команди

Операційні та кадрові ризики пов'язані з людськими ресурсами, процедурною спроможністю, часом, навантаженням, технікою, логістикою та інституційною пам'яттю.

Організація визнає, що робота в умовах повномасштабної війни, взаємодія з дітьми, вразливими групами, громадами, екологічними ризиками, кризовими ситуаціями та донорськими зобов'язаннями може створювати значне емоційне, психологічне й професійне навантаження на команду, волонтерів, консультантів і партнерів.

Організація розглядає добробут команди як частину управління ризиками та обов'язку турботи. Ризики перевантаження, вигорання, вторинної травматизації, хронічного стресу, роботи під час обстрілів, втрати мотивації або надмірної залежності від однієї особи мають враховуватися під час планування діяльності.

- реалістичне планування навантаження і строків;
- ротація завдань під час інтенсивних або емоційно складних періодів;
- можливість короткої паузи після складних польових, дитячих або кризових активностей;
- внутрішні розмови підтримки після складних інцидентів;
- перенаправлення до професійної психологічної або психосоціальної підтримки, якщо така доступна;
- недопущення культури «працювати попри все» у випадках, коли існує ризик для здоров'я, безпеки або якості роботи;
- фіксація уроків щодо навантаження команди у Журналі уроків або Реєстрі ризиків.

14. Страхування, безпека учасників і захист активів

Організація визнає, що страхування може бути важливим інструментом зменшення ризиків під час польових активностей, заходів із дітьми, роботи волонтерів, поїздок, використання обладнання або реалізації донорських проєктів.

- страхування учасників або волонтерів від нещасних випадків під час польових заходів, поїздок, таборів, навчальних візитів або активностей із підвищеним ризиком;
- страхування ключового обладнання, придбаного за кошти донорів або Організації;
- страхування відповідальності або інші види страхування, якщо цього вимагає донор, партнер, місце проведення заходу або характер діяльності;
- перевірка наявності страхування у транспортних, логістичних або інших підрядників, якщо це релевантно;
- документування рішення про страхування або обґрунтування, якщо страхування не застосовується.
- Для активностей із дітьми, волонтерами, польовими виїздами, роботою біля води, у природних зонах або з використанням цінного обладнання питання страхування має розглядатися під час оцінки ризиків і планування бюджету.

15. Ризики партнерств, субгрантів і підрядників

Партнерства, субгранти й підряди можуть створювати фінансові, репутаційні, етичні, екологічні, цифрові та safeguarding-ризики.

Оцінка партнерів, субгрантерів і підрядників має узгоджуватися з Політикою фінансового управління та закупівель, зокрема з підходом до оцінки спроможності субгрантера, лімітів фінансування, траншів, моніторингу, санкційної і репутаційної перевірки.

- партнер не має достатньої спроможності або не дотримується стандартів захисту дітей;
- неналежне використання коштів або слабке документування витрат;
- конфлікт інтересів;
- доступ партнера до персональних даних або дітей без належних гарантій;
- публікація некоректних даних або невиконання домовленостей.
- Мінімальні заходи: базова оцінка спроможності партнера або субгрантера; письмова угода; чіткі ролі, бюджет, строки, звітність і правила повернення коштів; перевірка репутаційних і санкційних ризиків у потрібних випадках; моніторинг виконання.

16. Реєстр ризиків

Організація веде внутрішній Реєстр ризиків для суттєвих програмних, фінансових, безпекових, екологічних, цифрових і репутаційних ризиків. Реєстр ризиків переглядається щонайменше щоквартально для активних проектів або перед поданням важливого донорського звіту.

17. Реагування на інциденти та ескалація

Інцидент - це подія або ситуація, яка вже створила або може створити шкоду людям, дітям, довкіллю, даним, фінансам, репутації або діяльності Організації.

- негайно зупинити або обмежити активність, якщо є загроза безпеці.
- Забезпечити безпеку людей, дітей і команди.
- Повідомити керівника Організації або відповідальну особу.
- Зафіксувати інцидент.
- Оцінити рівень ризику.
- Визначити коригувальні дії.
- Повідомити донора, партнера або компетентний орган, якщо це потрібно.
- Задokumentувати уроки та оновити процедури за потреби.

Рівень інциденту	Приклад	Хто реагує
Низький	дрібна організаційна помилка, незначна затримка	відповідальний за активність
Середній	скарга учасника, технічний збій, незначний польовий ризик	відповідальна особа / керівник
Високий	ризик для дитини, значна фінансова помилка, конфлікт із громадою, витік даних	керівник Організації, відповідальна особа, профільна політика
Критичний	загроза життю, насильство, серйозне порушення закону, масштабний витік даних або шахрайство	керівник, керівний орган, донор, компетентні органи за потреби

18. Кризові комунікації під час серйозних інцидентів

У разі серйозного інциденту Організація прагне забезпечити швидку, точну, відповідальну та узгоджену комунікацію з учасниками, батьками, партнерами, донорами, громадою, медіа або компетентними органами.

Серйозними інцидентами можуть бути травма дитини або учасника, порушення safeguarding, значна безпекова подія, витік персональних даних, підозра шахрайства, серйозний конфлікт із громадою, значна екологічна шкода, негативна медійна увага або публікація помилкової інформації.

- одна відповідальна особа координує зовнішню комунікацію;
- інформація перевіряється перед поширенням;
- не публікуються персональні дані, дані дітей, медичні деталі або чутлива інформація;
- батьки, партнери або донори інформуються відповідно до характеру інциденту та договірних вимог;
- комунікація не має створювати паніку, стигму, звинувачення без доказів або додаткові ризики;
- якщо питання стосується дитини або вразливої особи, пріоритет має Політика захисту дітей і вразливих груп;

- керівник Організації або визначена ним особа є основним речником під час серйозних інцидентів; інші члени команди, волонтери або партнери не надають публічних коментарів без погодження.

19. Безперервність діяльності

Організація прагне підтримувати безперервність ключових функцій навіть в умовах війни, перебоїв електропостачання, інтернету, кадрових змін або надзвичайних ситуацій.

- безпека дітей і учасників;
- доступ до фінансових і юридичних документів;
- зв'язок із донорами й партнерами;
- доступ до банківських рахунків;
- збереження даних і звітів;
- робота сайту та ключових комунікацій;
- виконання донорських зобов'язань;
- захист персональних даних.

20. Зв'язок із моніторингом, оцінкою, підзвітністю та навчанням

Управління ризиками є частиною системи моніторингу, оцінки, підзвітності та навчання Організації. Ризики мають відстежуватися під час реалізації проєктів, враховуватися у звітах, аналізуватися під час оцінок, розглядатися під час навчальних і рефлексійних сесій, вноситися до журналу уроків і впливати на планування наступних активностей.

Журнал уроків і Реєстр ризиків переглядаються щорічно перед плануванням наступного року. Зміни, зроблені на основі уроків, документуються.

21. Ролі та відповідальність

Роль	Відповідальність
Керівник Організації	Загальний нагляд за управлінням ризиками, рішення щодо високих і критичних ризиків, ескалація, комунікація з донорами або партнерами за потреби.
Відповідальна особа з управління ризиками	Ведення Реєстру ризиків, координація оцінки ризиків, контроль виконання запобіжних і коригувальних дій.
Програмна команда	Виявлення ризиків у проєктах, заповнення чеклистів, документування уроків, повідомлення про інциденти.
Відповідальні за заходи	Безпека учасників, маршрути, інструктажі, згода, перша допомога, польові чеклисти.
Відповідальна особа з моніторингу, оцінки, підзвітності та навчання	Включення ризиків у моніторинг, звітність, оцінку, навчання та журнал уроків.
Фінансова відповідальна особа / бухгалтер	Фінансові, закупівельні, валютні, авансові та документальні ризики.
Комунікаційна команда	Репутаційні ризики, перевірка фактів, відповідальна публікація даних, фото, історій і матеріалів.
Партнери та підрядники	Дотримання відповідних політик, повідомлення про ризики й інциденти, участь у коригувальних діях.

22. Перегляд політики

Політика переглядається щорічно або раніше у разі зміни безпекового контексту, зміни законодавства, нових донорських вимог, суттєвого інциденту, зміни програмної діяльності, запуску нового напрямку або фреймворку, результатів аудиту, оцінки або моніторингу, суттєвих скарг або звернень, оновлення пов'язаних політик.

Оновлення Політики документується із зазначенням версії, дати та суті змін.

Затверджено: Керівник Організації  / Микола Скиданюк /

Дата: 13.06.2026

Додатки**Додаток 1. Реєстр ризиків**

Дата	Опис ризику	Категорія	Рівень	Ймовірність	Вплив	Заходи	Відпові дальній	Строк	Статус	Уроки

Додаток 2. Теплова карта ризиків

Ймовірність / Вплив	Низький вплив	Середній вплив	Високий вплив	Критичний вплив
Низька ймовірність	Низький	Низький	Середній	Високий
Середня ймовірність	Низький	Середній	Високий	Високий
Висока ймовірність	Середній	Високий	Високий	Критичний
Дуже висока ймовірність	Середній	Високий	Критичний	Критичний

Додаток 3. Чеклист оцінки ризику перед активністю

- Чи залучені діти або вразливі групи?
- Чи потрібна згода батьків, школи, громади або партнера?
- Чи є ризики для безпеки, здоров'я або доступності?
- Чи перевірено маршрут, погоду, укриття і зв'язок?
- Чи є ризик для води, берегів, рослинності, тварин або природоохоронної території?
- Чи збираються персональні дані, фото, відео або геодані?
- Чи є ризик публікації чутливої інформації?
- Чи є фінансові або закупівельні ризики?
- Чи є конфлікт інтересів?
- Чи потрібна додаткова перевірка партнера або підрядника?
- Чи є план реагування на інцидент?
- Чи активність дозволена / потребує змін / переноситься / скасовується?

Додаток 4. Форма повідомлення про інцидент

Поле	Заповнення
Дата і час	
Місце	
Хто повідомив	
Тип інциденту	
Короткий опис	
Чи є ризик для дітей або вразливих груп	
Чи є ризик для здоров'я або безпеки	
Чи є ризик для даних або репутації	
Негайні дії	
Відповідальна особа	
Чи потрібна ескалація	
Коригувальні дії	
Статус	
Дата закриття	

Додаток 5. Матриця ризиків Карпатської ініціативи

Категорія ризику	Приклад	Рівень	Запобіжні заходи	Відповідальний
Воєнний / безпековий	повітряна тривога під час заходу	критичний	зупинка активності, укриття, перенесення заходу	відповідальний за захід / керівник
Захист дітей	фото або участь дитини без належної згоди	високий	форми згоди, інструктаж, контроль публікацій	відповідальна особа / керівник
Екологічний	шкода берегу, рослинності або природному об'єкту	середній / високий	польовий чеклист, маршрут, "не залишати слідів"	відповідальний за активність

Дані	публікація персональних або чутливих геоданих	високий	очищення даних, контроль доступу, перевірка перед публікацією	відповідальна особа з даних
Фінансовий	відсутні документи або порушена закупівля	середній / високий	фінансова політика, закупівельний файл, внутрішній контроль	фінансова особа
Репутаційний	неперевірені екологічні твердження	високий	перевірка фактів, обережна мова, анти-маніпуляційна політика	комунікаційна команда
Операційний	відсутність ключової особи або технічний збій	середній	резервна особа, резервні копії, план перенесення	керівник / команда
Партнерський	партнер не має достатньої спроможності	середній / високий	оцінка спроможності, договір, моніторинг	керівник / програмна команда

Додаток 6. Мінімальний план безперервності діяльності

Критична функція	Ризик	Резервне рішення	Власник відновлення	Орієнтовний строк відновлення
Банківські операції	втрата доступу або недоступність відповідальної особи	резервна уповноважена особа / зв'язок із банком	керівник / фінансова особа	1-3 робочі дні
Донорська звітність	втрата документів або дедлайн	хмарний архів / календар звітності	керівник / MEAL-відповідальна особа	до 5 робочих днів
Дані KoboToolbox / таблиці	відсутність інтернету або втрата доступу	локальне збереження / резервна копія	MEAL-відповідальна особа	1-5 робочих днів
Заходи з дітьми	тривога, погода, відсутність укриття	перенесення / укриття / альтернативний формат	відповідальний за захід	негайно / до 24 годин
Комунікація	блокування сайту або соціальних мереж	резервний канал / email / партнерська комунікація	комунікаційна особа / керівник	до 24-48 годин
Ключове обладнання	пошкодження, втрата або недоступність	реєстр активів / страхування за потреби / резервне обладнання	відповідальна особа за активи	1-10 робочих днів

Додаток 7. Чеклист добробуту команди після складної активності або інциденту

- Чи була активність пов'язана з підвищеним стресом, безпековою загрозою, роботою з дітьми або кризою?
- Чи потрібна коротка командна розмова після події?
- Чи є ознаки перевантаження, виснаження або вторинної травматизації?
- Чи потрібно перерозподілити або відтермінувати завдання?
- Чи доступна психологічна або психосоціальна підтримка?
- Чи потрібно зафіксувати урок у Журналі уроків або Реєстрі ризиків?

Додаток 8. Мінімальний чеклист кризової комунікації

- Визначено відповідальну особу за комунікацію.
- Факти перевірені перед поширенням.
- Не публікуються персональні дані, дані дітей, медичні деталі або чутлива інформація.
- Батьки, донори, партнери або компетентні органи інформуються відповідно до характеру інциденту.
- Повідомлення не створює паніки, стигми або звинувачень без доказів.
- Команда знає, що публічні коментарі надає лише визначений речник.

Concise English Reference Summary

The Ukrainian version of this Policy is the primary and official working version approved by the Organization. This English summary is provided for donor review and communication with international partners.

Youth Public Environmental Organization “Our Home - Manyava” applies a risk management system to identify, assess, mitigate, monitor and document risks related to children and vulnerable groups, environmental and field activities, small rivers, water safety, digital tools, personal data, geodata, finance, procurement, partnerships, subgrants, reputation, war-related safety, staff and volunteer well-being, insurance considerations, crisis communications, donor compliance and business continuity.

The Policy is aligned with the Carpathian Resilience Initiative 2026-2028 and linked to the Organization’s Safeguarding Policy, Privacy Policy, Anti-Corruption Policy, Environmental, Climate and Community Resilience Policy, Financial Management and Procurement Policy, MEAL Policy and Digital Governance and AI Ethics Policy.

The Organization maintains a risk register, applies proportional risk screening before activities, escalates high and critical risks, documents incidents and lessons learned, applies crisis communication rules, and integrates risk management into monitoring, evaluation, accountability and learning.

Approved by: Head of the Organization  / Mykola Skydaniuk /

Date: 13.06.2026