БЛАГОДІЙНА ОРГАНІЗАЦІЯ
«БЛАГОДІЙНИЙ ФОНД
«ДОБРОБУТ УКРАЇНИ»
ЄДРПОУ 40234987
61018, Україна, м. Харків,
вул. Отакара Яроша, 61-А, к. 10

CHARITABLE ORGANIZATION
«CHARITABLE FOUNDATION
«EUDEMONY OF UKRAINE»
№ 40234987
Otakara Yarosha street 61-A ap. 10 Kharkiv
Ukraine 61018

№18 від 28.08.2025

Н А К А З

Про затвердження Політики оцінки та управління ризиками

З метою забезпечення безпечної, відповідальної та безперервної діяльності Благодійної організації "Благодійний Фонд "Добробут України", впровадження підходів до оцінки, мінімізації та моніторингу ризиків, а також забезпечення дотримання внутрішніх процедур Організації, керуючись Статутом

НАКАЗУЮ:

1. Затвердити Політику оцінки та управління ризиками в Благодійної організації «Благодійного фонду "Добробут України» (додається).
2. Контроль за виконанням даного наказу покласти на Виконавчого директора Організації.

Голова Правління **Вікторія ПРЕОБРАЖЕНСЬКА**

З Наказом ознайомлені:

Виконавчий директор
Антон БІЛЮК

Дата: «28» серпня 2025 р.

ЗАТВЕРДЖЕНО
Наказом Голови Правління

БО “БФ «ДОБРОБУТ УКРАЇНИ»
від 28.08.2025 №18

ПОЛІТИКА ОЦІНКИ ТА УПРАВЛІННЯ РИЗИКАМИ БЛАГОДІЙНОЇ ОРГАНІЗАЦІЇ «БЛАГОДІЙНИЙ ФОНД “ДОБРОБУТ УКРАЇНИ”

м. Київ – 2025 рік

tel.+380954152277 https://cfdobrobutua.weblium.site e-mail: info@dobrobutua.org
Р/р UA613515330000026007052221644 в ПАТ КБ «Приват Банк» у м. Київ МФО 351533

1. ЗАГАЛЬНІ ПОЛОЖЕННЯ

1.1. Ця Політика визначає основні принципи, підходи та процедури оцінки, управління та моніторингу ризиків у діяльності БО “БФ "ДОБРОБУТ УКРАЇНИ" (далі - Організація).

1.2. Метою Політики є забезпечення безпечної та відповідальної реалізації програмної діяльності, своєчасне виявлення, оцінка та мінімізація ризиків, захист працівників/ць, волонтерів/ок, консультантів/ок, бенефіціарів та партнерів Організації, підтримка безперервності діяльності Організації, забезпечення дотримання вимог донорів, законодавства України та внутрішніх політик Організації.

1.3. Ця Політика поширюється на:

- працівників/ць Організації;
- консультантів/ок;
- волонтерів/ок;
- надавачів/чок послуг;
- стажерів/ок;
- членів керівних органів;
- інших осіб, залучених до діяльності Організації.

Усі зазначені особи зобов’язані дотримуватися положень цієї Політики в межах своєї діяльності та співпраці з Організацією.

1.4. Організація визнає, що управління ризиками є невід’ємною складовою гуманітарної, соціальної, освітньої та польової діяльності.

1.5. Організація застосовує ризик-орієнтований підхід під час:

- планування програмної діяльності;
- організації польових виїздів;
- роботи з дітьми та іншими вразливими групами;
- управління персоналом;
- роботи з персональними даними;
- фінансового управління;
- взаємодії з партнерами та підрядниками.

2. ОСНОВНІ ПРИНЦИПИ УПРАВЛІННЯ РИЗИКАМИ

2.1. Організація дотримується принципів безпеки, превентивності, конфіденційності, відповідальності, пропорційності, недискримінації, safeguarding та duty of care у процесі планування та реалізації своєї діяльності, управління персоналом, організації польових виїздів, роботи з бенефіціарами та взаємодії з партнерами.

2.2. Організація прагне своєчасно виявляти потенційні ризики, оцінювати їх можливий вплив та впроваджувати розумні й пропорційні заходи для попередження, мінімізації або реагування на такі ризики з урахуванням безпекового контексту, потреб діяльності та наявних ресурсів.

2.3. Управління ризиками здійснюється з урахуванням контексту діяльності Організації, рівня ризику, наявних ресурсів та безпекової ситуації.

2.4. Усі працівники/ці та інші залучені особи несуть відповідальність за дотримання вимог безпеки та повідомлення про відомі ризики або інциденти.

3. КАТЕГОРІЇ РИЗИКІВ

3.1. У межах своєї діяльності Організація може здійснювати оцінку різних категорій ризиків, які можуть впливати на безпеку персоналу, бенефіціарів, партнерів, реалізацію програмної діяльності, репутацію Організації та безперервність роботи.
3.2. До безпекових ризиків можуть належати ризики, пов’язані з бойовими діями, обстрілами, мінною небезпекою, нестабільною безпековою ситуацією, пересуванням у небезпечних районах, польовими виїздами, а також потенційні ризики для працівників/ць, волонтерів/ок, партнерів та бенефіціарів Організації.
3.3. Організація також враховує safeguarding ризики, зокрема ризики для дітей та інших вразливих груп населення, ризики сексуальної експлуатації та наруги (PSEA), психологічного або фізичного насильства, порушення етичних принципів, неналежної поведінки або зловживання владою.
3.4. До операційних ризиків можуть належати ризики, пов’язані зі зривом програмної діяльності, нестачею персоналу, логістичними труднощами, технічними несправностями, перебоями зв’язку, електропостачання або іншими обставинами, які можуть вплинути на реалізацію діяльності Організації.
3.5. Організація може оцінювати фінансові ризики, включаючи ризики нецільового використання коштів, шахрайства, корупційних дій, фінансових помилок, неналежного ведення документації або інших порушень фінансових процедур.
3.6. До репутаційних ризиків можуть належати порушення етичних стандартів, поширення неправдивої або некоректної інформації, неналежна поведінка представників Організації або інші дії, які можуть негативно вплинути на довіру до Організації.
3.7. Організація також враховує ризики, пов’язані із захистом персональних даних та інформаційною безпекою, зокрема ризики витоку персональних даних, втрати документів, несанкціонованого доступу до інформації, кібератак, використання незахищених каналів зв’язку або неналежного зберігання інформації.
3.8. До ризиків для добробуту персоналу можуть належати професійне вигорання, вторинна травматизація, надмірне робоче навантаження, психологічне виснаження, тривалий стрес або інші фактори, що можуть впливати на фізичний та емоційний стан працівників/ць та інших залучених осіб.

4. ОЦІНКА РИЗИКІВ

4.1. Організація може проводити оцінку ризиків перед початком реалізації проєктів, організацією заходів, польових виїздів, діяльності у нових громадах або

локаціях, а також у разі зміни безпекової ситуації, виникнення інцидентів або появи нових ризиків.
4.2. Оцінка ризиків може включати визначення потенційних ризиків, аналіз ймовірності їх виникнення та можливого впливу, визначення заходів пом'якшення ризиків, а також розподіл відповідальності за впровадження необхідних заходів безпеки або реагування.
4.3. Для проведення оцінки ризиків Організація може використовувати Risk Assessment Forms, плани польових пересувань, безпекові брифінги, внутрішні чек-листи, процедури погодження виїздів, а також інші внутрішні інструменти оцінки ризиків та безпеки.
4.4. Для діяльності, пов'язаної з підвищеним рівнем ризику, Організація може застосовувати додаткові заходи безпеки, погодження, моніторингу або обмеження діяльності відповідно до внутрішніх процедур та актуального безпекового контексту.

5. ЗАХОДИ З МІНІМІЗАЦІЇ РИЗИКІВ

5.1. З метою мінімізації ризиків Організація може впроваджувати безпекові інструктажі, обмеження або заборону виїздів у небезпечні райони, використання засобів зв'язку, контроль доступу до інформації, використання захищених електронних систем, навчання персоналу, супервізійну та психологічну підтримку, процедури safeguarding та PSEA, а також плани евакуації або реагування на інциденти.
5.2. Організація залишає за собою право призупинити, перенести або скасувати діяльність, польові виїзди чи заходи у разі надмірного рівня ризику, загрози безпеці або неможливості забезпечення належних заходів захисту.

6. РОЛІ ТА ВІДПОВІДАЛЬНІСТЬ

6.1. Голова Правління та керівництво Організації здійснюють загальний нагляд за процесами управління ризиками, сприяють впровадженню безпечних підходів до діяльності та забезпечують підтримку внутрішніх процедур безпеки.
6.2. Офіцер/ка з безпеки координує процеси безпекової оцінки, здійснює моніторинг безпекової ситуації, надає рекомендації щодо безпеки, бере участь у розгляді польових пересувань та інцидентів, а також може ініціювати додаткові заходи безпеки або перегляд ризиків.
6.3. Керівники/ці проєктів та команд повинні враховувати ризики під час планування діяльності, забезпечувати дотримання процедур безпеки, підтримувати належну комунікацію з командами та своєчасно повідомляти про нові ризики або інциденти.
6.4. Працівники/ці, волонтери/ки, консультанти/ки та інші залучені особи зобов'язані дотримуватися вимог безпеки, брати участь у необхідних інструктажах, повідомляти про ризики, інциденти або порушення, а також сприяти створенню безпечного робочого середовища.

7. РЕАГУВАННЯ НА ІНЦИДЕНТИ

7.1. У разі виникнення інциденту Організація може здійснювати оцінку ситуації, вживати заходів для забезпечення безпеки людей, повідомляти відповідальних осіб, документувати інцидент, впроваджувати заходи реагування та переглядати наявні процедури або оцінку ризиків.

7.2. Працівники/ці та інші залучені особи зобов'язані своєчасно повідомляти про безпекові інциденти, порушення safeguarding, ризики для дітей, випадки PSEA, витоки персональних даних, суттєві порушення безпеки або інші ризики, що можуть вплинути на діяльність Організації чи безпеку людей.

7.3. Організація сприяє створенню безпечного середовища для повідомлення про ризики, інциденти або порушення та не допускає переслідування осіб, які добросовісно повідомили про потенційні або фактичні ризики чи порушення.

8. КОНФІДЕНЦІЙНІСТЬ ТА ЗАХИСТ ДАНИХ

8.1. Інформація, отримана під час оцінки ризиків, розгляду інцидентів або здійснення заходів реагування, повинна оброблятися конфіденційно, з урахуванням принципу необхідності доступу до інформації.

8.2. Документи та матеріали, що містять персональні дані або іншу чутливу інформацію, повинні зберігатися та оброблятися відповідно до внутрішніх політик Організації щодо захисту персональних даних, інформаційної безпеки та конфіденційності.

9. НАВЧАННЯ ТА ПІДВИЩЕННЯ ОБІЗНАНОСТІ

9.1. Організація може проводити навчання, інструктажі, інформаційні сесії або інші заходи для працівників/ць та залучених осіб з питань управління ризиками, безпеки, safeguarding, PSEA, інформаційної безпеки, реагування на інциденти, психологічної безпеки та профілактики професійного вигорання.

10. ПЕРЕГЛЯД ПОЛІТИКИ

10.1. Політика може переглядатися та оновлюватися за потреби у разі змін законодавства України, безпекового контексту, структури Організації, характеру діяльності або вимог донорів.

10.2. Організація може оновлювати внутрішні процедури, форми та інструменти управління ризиками відповідно до актуальних потреб діяльності та практичного досвіду реалізації програм.

11. ПРИКІНЦЕВІ ПОЛОЖЕННЯ

11.1. Ця Політика набирає чинності з моменту її затвердження Головою Правління Організації.

11.2. Усі працівники/ці, волонтери/ки, консультанти/ки та інші залучені особи повинні бути ознайомлені з цією Політикою та дотримуватися її положень у межах своєї діяльності.

Голова Правління  **Вікторія ПРЕОБРАЖЕНСЬКА**

З Політикою ознайомлені:

Виконавчий директор
Антон БІЛЮК

Дата: «28» серпня 2025р.

tel.+380954152277 https://cfdobrobutua.weblium.site e-mail: info@dobrobutua.org
Р/р UA613515330000026007052221644 в ПАТ КБ «Приват Банк» у м. Київ МФО 351533