

ПОЛІТИКА БЕЗПЕКИ

Громадської організації «Центр досліджень і сприяння реформ» (ГО «ЦДСР»)

1. Загальні положення та нормативно-правова база

Політика безпеки Громадської організації «Центр досліджень і сприяння реформ» (надалі — ГО «ЦДСР») є засадничим внутрішнім документом, який визначає ключові принципи, правила, стандарти та алгоритми дій задля гарантування безпеки життя, фізичного та ментального здоров'я команди, а також збереження матеріальних, інформаційних та цифрових активів ГО «ЦДСР».

Цей документ розроблено на підставі статті 130 Кодексу цивільного захисту України, чинного законодавства у сфері охорони праці, цивільного захисту цивільного населення та міжнародних стандартів гуманітарної діяльності й антикризового управління. Політика враховує специфіку діяльності ГО «ЦДСР» як експертно-аналітичного центру, що здійснює незалежні дослідження, консалтинг та реалізацію проєктів в умовах воєнного стану, військових загроз та підвищених операційних ризиків.

Дія цієї Політики поширюється на всіх членів ГО «ЦДСР», штатних співробітників, залучених експертів, волонтерів, стажерів та підрядників, які виконують завдання від імені або в інтересах ГО «ЦДСР» як на території офіційних локацій, так і дистанційно або під час польових досліджень та закордонних відряджень.

2. Управління безпекою та розподіл відповідальності

Загальне стратегічне керівництво та контроль за дотриманням Політики безпеки здійснює Голова Правління та Виконавчий директор ГО «ЦДСР». До їхніх обов'язків належить ухвалення рішень про призупинення офлайн-діяльності, евакуацію, зміну формату роботи на виключно дистанційний, а також

виділення необхідних ресурсів для забезпечення інструментів безпеки.

Кожен керівник проєкту або польової дослідницької групи є безпосередньо відповідальним за безпеку підпорядкованої команди. Він зобов'язаний провести первинний інструктаж перед початком робіт чи відряджень, моніторити поточну безпекову ситуацію в регіоні виконання завдань та забезпечити наявність засобів зв'язку та першої допомоги.

Усі залучені спеціалісти та волонтери несуть персональну відповідальність за суворе дотримання вимог цієї Політики, негайне реагування на сигнали тривоги та невідкладне сповіщення керівництва про будь-які інциденти чи потенційні загрози.

3. Фізична безпека та алгоритм дій під час воєнних загроз

3.1. Дії під час сигналу «Повітряна тривога» або загрози ракетного/артилерійського обстрілу:

- При отриманні сигналу тривоги через офіційні канали сповіщення або мобільні додатки всі співробітники та волонтери, які перебувають у приміщеннях ГО, зобов'язані негайно припинити роботу, закрити вікна, вимкнути електроприлади та залишити будівлю.

- Потрібно якнайшвидше переміститися до найближчого офіційного укриття або сертифікованого бомбосховища. Напрямок руху та локація найближчих сховищ мають бути чітко зазначені на інформаційних стендах у приміщеннях ГО.

- У разі неможливості швидко дістатися до капітального укриття, слід застосувати правило «двох стін» або сховатися у внутрішніх приміщеннях без вікон (коридори, санвузли) подалі від скляних конструкцій.

- Категорично заборонено підходити до вікон, проводити фото- чи відеозйомку роботи засобів ППО або місць влучань.

3.2. Особливості дій під час хімічної або радіаційної небезпеки:

- Якщо сигнал про хімічну чи радіаційну атаку застав команду

всередині приміщення, необхідно негайно закрити всі вікна, двері, вентиляційні отвори та ущільнити їх подручними засобами (вологою тканиною, скотчем), щоб мінімізувати притік зовнішнього повітря.

- Враховуючи, що більшість хімічних бойових речовин важчі за повітря і осідають на землю, за можливості слід піднятися на вищі поверхи будівлі, обравши кімнату з мінімальною кількістю вікон.

- Якщо небезпека застала співробітника під час пересування на службовому чи особистому автомобілі під час виконання завдань ГО, необхідно з'їхати на узбіччя, щоб не блокувати рух спецтранспорту, вимкнути двигун, щільно закрити вікна та перекрити вентиляційні канали й кондиціонер, які втягують повітря ззовні.

- Слід увімкнути засоби зв'язку (радіо, офіційні державні інтернет-канали) для отримання інструкцій від ДСНС щодо подальшої евакуації чи виходу з ураженої зони. Заборонено вживати воду чи їжу, що могли зазнати впливу шкідливих речовин.

4. Безпека польових досліджень та відряджень

Оскільки ГО «ЦДСР» проводить соціологічні та ринкові дослідження, збір первинних даних та моніторинг реформ безпосередньо у громадах, планування польових виїздів здійснюється за особливим протоколом безпеки:

Етап проєкту	Обов'язкові безпекові заходи та вимоги
Підготовка та планування	Обов'язковий моніторинг безпекової ситуації у цільовій громаді (рівень мінної небезпеки, інтенсивність обстрілів). Погодження маршрутів із місцевими органами військової адміністрації або ДСНС. Перевірка наявності

Етап проєкту	Обов'язкові безпекові заходи та вимоги
	сертифікованих укриттів на шляху прямування та в місцях проведення інтерв'ю чи зустрічей.
Екіпірування групи	Кожна дослідницька група забезпечується укомплектованою тактичною аптечкою першої допомоги, павербанками високої ємності, індивідуальними ліхтарями та засобами надійного зв'язку. Для роботи у зонах підвищеного ризику (прифронтові чи деокуповані території) за потреби залучаються додаткові засоби захисту.
Комунікаційний протокол	Встановлення чітких графіків зв'язку (Check-in). Дослідники зобов'язані виходити на зв'язок із координатором проєкту в ГО «ЦДСР» за заздалегідь визначеними годинами (наприклад, кожні 3–4 години) та негайно звітувати про прибуття у фінальну точку маршруту.

5. Інформаційна та кібербезпека

Експертна аналітика та результати досліджень потребують суворого захисту. Кібербезпека ГО «ЦДСР» включає такі імперативи:

- **Конфіденційність респондентів:** Усі первинні соціологічні дані, персональна інформація учасників опитувань та фокус-груп мають бути повністю знеособлені (анонімізовані) та зберігатися у зашифрованому вигляді для унеможливлення їхнього витоку чи несанкціонованого доступу третіх осіб.

- **Корпоративні комунікації:** Уся офіційна, фінансова та проєктна переписка ведеться виключно через офіційні корпоративні електронні скриньки ГО «ЦДСР». Заборонено передавати службову інформацію, паролі або бази даних через незахищені приватні месенджери чи особисту пошту.

- **Парольна гігієна та автентифікація:** Для доступу до корпоративних хмарних сховищ, баз даних та облікових записів є обов'язковим використання складних унікальних паролів та підключення двофакторної автентифікації (2FA). Співробітники зобов'язані регулярно оновлювати програмне забезпечення на робочих пристроях та уникати використання публічних незахищених Wi-Fi мереж без підключення VPN.

6. Психологічна безпека та перша психологічна допомога

Ураховуючи високий рівень стресу, роботу у прифронтових зонах та загальні виклики воєнного стану, ГО «ЦДСР» розглядає ментальне здоров'я як невід'ємну частину загальної системи безпеки.

ГО «ЦДСР» використовує внутрішню фахову експертизу в сфері психології комунікації та коучингу для запобігання професійному вигоранню команди, створення атмосфери психологічної стійкості, формування внутрішньої опори та надання першої психологічної допомоги у кризових ситуаціях. Будь-які прояви психологічного тиску, мобінгу чи ігнорування емоційного перевантаження є неприпустимими.

7. Порядок ознайомлення, тренінги та актуалізація Політики

Ця Політика безпеки затверджується рішенням Правління ГО «ЦДСР» та переглядається щонайменше один раз на рік або частіше у разі суттєвих змін безпекової чи нормативно-правової ситуації в країні.

Ознайомлення з Політикою є обов'язковим елементом процедури адаптації (онбордингу) для всіх нових співробітників, експертів та волонтерів. ГО «ЦДСР» регулярно проводить практичні тренінги, інструктажі з тактичної медицини, цивільного захисту та кібербезпеки для підтримання високого рівня готовності

команди до реагування на надзвичайні ситуації.

З Політикою безпеки ознайомлений(а) та зобов'язуюсь суворо дотримуватися її положень:

ПІБ:

Посада / Роль в ГО «ЦДСР»:

Дата: «___» _____ 20__ р. Підпис: _____