ГРОМАДСЬКА СПІЛКА
МЕРЕЖА ПРАВОВОГО РОЗВИТКУ

ГРОМАДСЬКА СПІЛКА
«МЕРЕЖА ПРАВОВОГО РОЗВИТКУ»
LEGAL DEVELOPMENT NETWORK

ldn.org.ua
office@ldn.org.ua
facebook.com/legaldnetwork

ЗАТВЕРДЖЕНО
Рішенням Правління
Громадської спілки
«Мережа правового розвитку»
Протокол
№ 1 від «20» січня 2025 року

БЕЗПЕКОВА ПОЛІТИКА

Безпека членів громадських організацій (далі — члени Мережі), що входять до Громадської спілки "Мережа правового розвитку" (далі — Мережа) — одна із основних відповідальностей нашої організації. Ми зобов'язуємося дбати про безпеку нашої команди, членських організацій, бенефіціарів та партнерів, залучених до реалізації спільних проєктів та ініціатив.

Метою цієї Політики безпеки є визначення принципів та підходів для створення безпечного середовища (фізичного, інформаційного, психологічного, інтелектуального тощо).

Дія цієї політики поширюється на усіх членів Мережі, співробітників, партнерів, стейкхолдерів, бенефіціарів, підрядників, осіб, закріплених контрактами з ГС “Мережа правового розвитку” на професійній чи іншій основі, у всіх формах співпраці, в тому числі під час виїздів в громади.

ОСНОВНІ ПРИНЦИПИ ЗАХИСТУ І БЕЗПЕКИ

Поняття безпеки є складновизначеним та має особливості для кожного члена Мережі. Ми користуємось наступним узагальненням: **Безпека — це стан захищеності людини, організації або системи від загроз чи ризиків, які можуть призвести до шкоди або втрат.**

В своїй діяльності ми дотримуємось наступних принципів безпеки:

Пріоритетність життя та здоров’я. Безпека є найголовнішим пріоритетом Мережі. Кожен має уникати потрапляння в ситуації з надмірним ризиком, аргументуючи це метою виконання програмної/проєктної діяльності або захисту майна.

Особиста відповідальність. Кожен має усвідомлювати особисту відповідальність за свою безпеку та має не ризикувати своїм життям. Цей принцип стосується ситуацій, коли перед людиною стоїть моральний вибір між ненаданням допомоги чи ризиком.

Незаподіяння шкоди іншим. Кожен має чітко усвідомлювати наслідки, які можуть бути спричинені його/її діями та виключати можливість заподіяння загрози життю та здоров’ю іншим, як наслідок особистої безвідповідальності.

Гнучке безпекове управління. Менеджмент програм відбувається у відповідності до обставин, регіональних особливостей та оточення. Планування, підготовка та імплементація будь-яких програм/проєктів Мережі має здійснюватися тільки з урахуванням ретельного аналізу ризиків та необхідних умов безпеки, що відповідають контексту програмної (проєктної)діяльності.

Безпека та добробут персоналу. Керівники, менеджери, співробітники будь-якого рівня Мережі, мають приділяти особливу увагу піклуванню про свій персонал; застосовувати інструменти визначення перевантаження та запобігання робочого вигорання; створювати та зберігати у колективі відносини взаємоповаги та доброзичливості.

Нульова толерантність за порушення правил безпеки. Нехтування правилами безпеки ставить під загрозу багатьох – як працівників Мережі, так представників членських організацій, бенефіціарів та партнерів.

СТРАТЕГІЯ БЕЗПЕКИ

Мережа забезпечує дотримання принципів неупередженості та нейтральності в усіх сферах діяльності, уникає підтримки будь-яких політичних чи збройних конфліктів, що відповідає стандартам гуманітарної сфери в Україні.

Оцінка ризиків: на постійній основі має проводиться аналіз рівня ризиків для членських організацій та персоналу, з урахуванням поточної ситуації в країні. Стратегія безпеки адаптується залежно від динаміки ризиків.

Захист без застосування насилля: Мережа уникає використання будь-яких збройних засобів захисту, зосереджуючись на методах превентивних заходів, навчанні, підвищенні обізнаності та дипломатичних механізмах вирішення конфліктів.

Партнерство та координація: спільна робота з партнерами, громадськими організаціями та місцевими стейкхолдерами для забезпечення безпечного середовища та координації заходів захисту без застосування примусових або військових заходів.

Моніторинг і оновлення: політика безпеки та відповідні протоколи переглядатимуться щорічно або при зміні обставин, які можуть впливати на діяльність Мережі, з метою постійного підвищення рівня безпеки та адаптації до нових викликів.

РОЛІ ТА ОБОВ'ЯЗКИ З ПИТАНЬ БЕЗПЕКИ

Виконавчий директор Мережі, а також керівники членських організацій, які входять в ГС "Мережа правового розвитку", несуть повну відповідальність за дотримання всіх норм чинного законодавства України щодо безпеки у відповідності до визначених сфер діяльності. Безпосередньо розглядають, затверджують та контролють впровадження і виконання політик, процедур та інструкцій щодо безпеки.

Керівники проєктів/програм відповідають за включення питання безпеки на всіх етапах програмного/проєктного циклу, а також за ситуаційну обізнаність працівників.

Менеджери/фахівці з питань безпеки є радниками керівника з питань безпеки персоналу, приміщень та програмної/проєктної діяльності. У співпраці з програмним та адміністративним менеджментом, відповідають за розробку та оновлення Протоколів (планів) безпеки. Здійснюють управління створеною, у відповідності до Планів, системою безпеки. Консультують/інформують усіх учасників щодо ситуаційної обізнаності в локаціях (населених пунктах), де планується проведення заходів.

Мережа активно працюватиме над формуванням такого середовища, при цьому кожен член Мережі несе відповідальність за власну безпеку та безпеку учасників, особливо під час воєнного стану. Також вважаємо, що кожен член команди зобов'язаний постійно дотримуватися основних правил безпеки та заохочувати до цього інших.

Політика розробляється та затверджується Правлінням Мережі за участю всіх зацікавлених сторін. Вона підлягають перегляду та оновленню щорічно або за необхідності, коли обставини, що впливають на діяльність Мережі, змінюються. Пропозиції та відгуки щодо змін до політики слід надсилати на вказану електронну адресу office@ldn.org.ua

Крім того, усі співробітники, підрядники, особи, закріплені контрактами з ГС "Мережа правового розвитку" на професійній або добровільній основі, виконуючи свої службові доручення, підпадають під дію політики безпеки. Політика не поширюється на членів сімей вищезгаданих

осіб, підрядників та працівників, закріплених контрактами з іншими НУО, які не входять в Мережу або установами. Тільки в ситуаціях, які загрожують життю, учасники мають певні повноваження нехтувати ними. Недотримання політики безпеки може призвести до закінчення співпраці з Мережею.

Всі учасники, на яких поширюється політика безпеки, мають право відмовитися від виїзних місій до територій з високим рівнем загрози, що не буде впливати на продовження їхньої співпраці Мережею. Вони також мають право залишати ті локації, де, за їхньою особистою оцінкою, існує загроза їхній безпеці або безпеці інших людей.

Коли, незважаючи на оцінку ризику, ситуація з ризиком безпеки погіршується, сягаючи за межі прийнятності, керівництво членської організації може ухвалити рішення щодо евакуації, яке не може бути оскаржене Мережею. Якщо і коли окрема особа більше не почувається комфортно в ситуації з ризиком безпеки, вона має право виїхати з громади (регіону), де впроваджується діяльність, раніше встановлених термінів за власні кошти та під власну відповідальність.

ТИПОВІ ПЛАНИ ДІЙ ТА ПРОТОКОЛИ БЕЗПЕКИ

Типові плани дій (ТПД) та **протоколи (плани) безпеки** мають схожі цілі, але вони відрізняються за своїм призначенням і рівнем деталізації:

Типові плани дій (ТПД):

- Мають на меті забезпечити чіткі інструкції для виконання конкретних завдань або дій в певних умовах (наприклад, виїзд до зони конфлікту).
- Зазвичай містять послідовність кроків, які повинні бути виконані у відповідь на певні загрози чи ситуації.
- Акцент робиться на конкретних діях для досягнення результату або уникнення ризиків, наприклад, як поводитися в разі евакуації або при втраті зв’язку.

Протоколи безпеки:

- Регламентують загальні принципи і стандарти безпеки для всієї організації або певних операцій.
- Описують заходи щодо зменшення ризиків, попередження загроз і захисту персоналу у різних умовах.
- Мають більш постійний характер і стосуються довготривалих правил, які всі учасники повинні дотримуватися (наприклад, вимоги щодо підготовки до поїздок, правила підтримки зв’язку, реагування на зміну рівня загроз).

Отже, ТПД фокусуються на конкретних ситуаціях і діях, тоді як протоколи (плани) безпеки є більш загальними і охоплюють стратегії захисту в ширшому контексті. З урахуванням регіональних особливостей Мережа рекомендує організаціям мати як ТПД (для регіонів, наближених до зони бойових дій) так і Протоколи безпеки (для регіонів з відносно безпечною ситуацією, але з наявним ризиком обстрілів).

Мережа не рекомендує своїм членам, працівникам та підрядникам здійснювати поїздки на тимчасово окуповані території. Мережа рекомендує своїм членам, співробітникам та підрядникам всебічно оцінювати ризики можливих поїздок на тимчасово окуповані території і в зону конфлікту, в тому числі на території максимально наближені до лінії бойових дій або українського кордону з рф.

Підрядники та співробітники на всіх рівнях організації повинні постійно відстежувати важливі політичні, соціальні, економічні та військові події в регіонах, де Мережа здійснює свою діяльність. Під час проведення виїзних операцій група та її керівник готують Типовий порядок дій (ТПД). Цей процес є динамічним і постійним, оскільки загрози та вразливість організації можуть змінюватися.

У разі зміни ситуації ризики для виїзних груп можуть зрости або знизитися, що вимагає відповідного коригування заходів захисту та безпеки.

Типовий план дій може складатися з наступних кроків[1]:

1. Оцінка ризиків

- Перед поїздкою всі учасники повинні провести детальну оцінку ризиків, включаючи аналіз поточної ситуації, рівня загроз та наявних безпекових умов на території.
- Використання даних із перевірених джерел (місцеві органи влади, міжнародні організації) для прийняття рішення про поїздку.

2. Підтримка зв'язку

- Учасники повинні забезпечити постійний зв'язок з координаторами Мережі та місцевими партнерами через захищені канали зв'язку.
- Встановлення регулярного графіку звітів та контактів під час перебування на небезпечній території.

3. План евакуації

- Кожен учасник повинен бути ознайомлений із планом евакуації на випадок загострення ситуації.
- Передбачити запасні маршрути виходу та транспортні засоби для швидкої евакуації в разі небезпеки.

4. Звітність

- Після завершення поїздки кожен учасник зобов’язаний подати короткий звіт про безпекову ситуацію, складнощі та проведені заходи.

ЗВІТУВАННЯ ПРО ВИПАДКИ НАДЗВИЧАЙНИХ СИТУАЦІЙ

Приклади інцидентів, які можуть бути класифіковані як надзвичайні ситуації в рамках діяльності Мережі:

Переслідування та загрозлива поведінка:

Напади на членів організації або їхні сім'ї.
Отримання погроз (включно з погрозами фізичного насильства чи вбивства) через електронні листи, дзвінки або особисті контакти.
Переслідування або залякування працівників чи підрядників на місці їх роботи або проживання.
Загрози насильницьких дій з боку місцевих угруповань або невідомих осіб.

Акти війни та збройні конфлікти:

Обстріли, ракетні удари або інші види атак на території, де проводиться діяльність організації.
Потрапляння в зону мінних полів або виявлення мін і вибухонебезпечних предметів.
Випадки стрілянини поблизу учасників або в районах їх перебування.

[1] Типові плани дій у різних ситуаціях, пов'язаних із ризиком для життя та здоров'я зібрані в наступному документі: https://docs.google.com/document/d/1QBS6d-oxX3WGOJ9Ney9WtV7bqUl_kLNFWUrK2B50uG8/edit?usp=sharing

Військові агресивні дії, такі як окупація території або силові акти, що загрожують життю та безпеці персоналу.

Крадіжки та розбій

Викрадення майна організації (техніки, транспорту, документів) або особистих речей учасників.
Озброєні напади або розбійні напади з метою заволодіння майном організації або працівників.
Злом офісних приміщень або місць проживання співробітників.

Шахрайські дії
Фінансове шахрайство, у вигляді підробки документів, фальшивих рахунків або зловживання службовими повноваженнями для заволодіння грошовими коштами організації або її працівників.
Використання соціальної інженерії для отримання доступу до конфіденційної інформації, зокрема через обман або маніпуляцію співробітниками, що може призвести до фінансових втрат або витоку даних.
Інтернет-шахрайство, включаючи фішинг, коли зловмисники намагаються отримати конфіденційну інформацію, такі як паролі або реквізити банківських карток, шляхом обману через електронні листи чи веб-сайти.

Викрадення та насильницькі дії:

Викрадення працівників, підрядників або членів їх сімей з метою викупу чи залякування.
Захоплення заручників або утримання людей проти їх волі.
Фізичне насильство або спроби насильства щодо співробітників чи партнерів Мережі.

Недопуск або обмеження пересування на блокпостах:

Відмова у пропуску через блокпости або інші пункти контролю, що створює перешкоди для виконання завдань (з урахуванням особливостей регіону та наявності дозвільних документів)
Загроза арешту або затримання на блокпостах.
Спроби конфіскації майна, документів або транспортних засобів на контрольно-пропускних пунктах.

Ці інциденти вимагають негайної реакції та активації дій, включаючи евакуацію, повідомлення правоохоронним органам та міжнародним правозахисним організаціям та моніторинговим місіям, підтримку зв'язку та інші заходи для захисту учасників, відповідно до ситуації.

Зазначений перелік надзвичайних ситуацій не є вичерпним, і кожен інцидент, що становить загрозу для безпеки учасників, майна чи репутації організації, має бути розглянутий як потенційна небезпека. Усі випадки, незалежно від їхнього характеру чи серйозності, повинні бути негайно повідомлені керівництву членських організацій та безпосередньо керівництву Мережі для своєчасного реагування та вжиття необхідних заходів.

Повідомити про будь-які порушення можна на електронну адресу office@ldn.org.ua чи у інший доступний спосіб.