«Затверджено»

Правлінням БО «Позитивні жінки»

Протокол від 16 червня 2025 року

Голова Правління

Стрижак Олена

ПОЛІТИКА
безпеки в умовах воєнного стану
Благодійної Організації
“ПОЗИТИВНІ ЖІНКИ”

КИЇВ 2025

ВСТУП

Зовнішня агресія російської федерації проти України - це спланована заздалегідь збройна агресія росії проти України, яка розпочалася 20 лютого 2014 року з військової операції збройних сил рф із анексією частини території України – Кримського півострова. 24 лютого 2022 року росія розпочала широкомасштабний військовий напад на Україну.

З першого дня агресії росія порушує правила ведення війни і норми міжнародного права та масово чинить воєнні злочини та злочини проти людяності, вбиваючи цивільних, руйнуючи інфраструктуру та депортуючи населення.

Широкомасштабний військовий напад на Україну змусив Благодійну Організацію "Позитивні жінки" (далі – Організацію) приділяти дедалі більше уваги безпеці — захисту учасниць, персоналу, залучених консультанток та фахівчинь, представниць, волонтерок, клієнток, партнерів тощо.

Організація розробила системний безпековий документ, який допомагає діяти на випередження та запобігати ризикам під час воєнного стану в Україні .

ТЕРМІНОЛОГІЯ:

Воєнний стан — це особливий правовий режим, що вводиться в Україні або в окремих її місцевостях у разі збройної агресії чи загрози нападу, небезпеки державній незалежності та територіальній цілісності. Він передбачає надання органам державної влади, військовому командуванню, військовим адміністраціям та органам місцевого самоврядування повноважень, необхідних для відвернення загрози, відсічі збройної агресії та гарантування національної безпеки, а також тимчасове, зумовлене загрозою, обмеження конституційних прав і свобод людини та громадянина, прав і законних інтересів юридичних осіб із зазначенням строку дії цих обмежень. Воєнний стан введений в Україні 24 лютого 2022 року.

Небезпека під час воєнного стану - це явища, викликані обставинами, пов'язаними із подіями воєнного стану (обстріли, окупація, повітряні тривоги та інше), які здатні завдати шкоди здоров'ю, життю, добробуту людини як відразу, так і в майбутньому.

Оцінка ризику небезпеки під час воєнного стану – це процес виявлення потенційних небезпек і оцінки відповідних ризиків. Він передбачає визначення потенційних джерел шкоди, аналіз ймовірності виникнення небезпеки та оцінку потенційних наслідків небезпеки.

Повітряна тривога – сигнал оповіщення населення про реальну загрозу атаки з повітря. Вмикається у разі ризику авіаудару або запуску ракет/шахедів у напрямку населеного пункту чи області.

1. Загальні Положення

1.1 Ця Політика визначає основні принципи та процедури забезпечення безпеки учасниць, персоналу, залучених консультанток та фахівчинь, представниць, волонтерок/ів, клієнток, партнерів, Організації в умовах зовнішньої агресії.

1.2. Безпека є найвищим пріоритетом для Організації. Всі рішення та дії повинні враховувати потенційні ризики та спрямовуватися на їх мінімізацію.

1.3. Ця Політика розроблена відповідно до чинного законодавства України, міжнародних гуманітарних принципів та найкращих практик у сфері безпеки некомерційних організацій.

1.4. Усі учасниці Організації, а також усі особи, закріплені контрактами з Організацією на професійній або добровільній основі, виконуючи свої службові доручення, підпадають під Політику та протоколи безпеки. Політика не поширюється на членів сімей вищезгаданих осіб, та на осіб, які не мають із Організацію жодних договірних відносин (трудових, цивільно-правових, волонтерських, статутних).

1.5. Люди є найвищим пріоритетом Організації. Політика та протоколи поширюються лише на людей, а не матеріальне майно і фінансові засоби.

1.6. Всі учасниці Організації, а також усі особи, закріплені контрактами з Організацією мають право залишати ті локації, де, за їхньою особистою оцінкою, існує загроза їхній безпеці або безпеці інших людей.

1.7. Дана Політика не передбачає охоплення всіх видів небезпек у життєдіяльності людини, а лише ті, які викликані подіями в державі під час воєнного стану.

2. Цілі Політики.

2.1. Забезпечення максимального рівня безпеки для всіх осіб, пов’язаних з діяльністю Організації.

2.2. Мінімізація ризиків травмування, загибелі щодо учасниць, персоналу, залучених консультанток та фахівчинь, представниць, волонтерок/ів, клієнток, партнерів.

2.3. Забезпечення безперервності діяльності Організації, наскільки це можливо в умовах зовнішньої агресії та воєнного стану.

2.4. Підвищення обізнаності з питань безпеки.

2.5. Реалізація в Організації правила: “Уникати, запобігати, діяти». Уникати — це розпізнавати небезпечні ситуації, оцінювати ризик і діяти так, щоб не потрапляти у них. Запобігати — це передбачати наслідки дій, щоб самим не створювати небезпечних ситуацій. Діяти — не розгубитися, знати, що і як робити”.

3. Основні Принципи Безпеки.

3.1. *Оцінка ризиків:* регулярний та систематичний аналіз потенційних загроз та вразливостей у місцях діяльності Організації.

3.2. *Запобіжні заходи:* впровадження проактивних заходів для зменшення ймовірності та наслідків безпекових інцидентів.
3.3. *Інформування та навчання:* забезпечення всіх інформацією та навчанням учасниць, персоналу, залучених консультанток та фахівчинь, представниць, волонтерок/ів, клієнток, партнерів з питань безпеки, першої допомоги та дій у надзвичайних ситуаціях.
3.4. *Дотримання процедур:* обов'язкове дотримання встановлених безпекових протоколів та інструкцій.
3.5. *Координація, співпраця та комунікація:* налагодження ефективної системи зв'язку та координації між усіма членкинями та членами команди. Організація співпрацює з відповідними державними органами, неурядовими організаціями та місцевими громадами для обміну інформацією та координації зусиль щодо забезпечення безпеки.
3.6. *Гнучкість та адаптивність:* здатність швидко реагувати на зміни в безпековій ситуації та адаптувати безпекові заходи відповідно до нових обставин.
3.7. *Неупередженість та нейтралітет:* Організація дотримується принципів неупередженості та нейтралітету в своїй діяльності, надаючи допомогу на основі потреб, без дискримінації за будь-якими ознаками. Це сприяє зменшенню ризиків для безпеки.
3.8. *Відповідальність:* чітке визначення ролей та відповідальності за забезпечення безпеки на всіх рівнях Організації.

4. Розробка, впровадження, відповідальність за виконання Політики та протоколів безпеки.

4.1. Політика та протоколи безпеки розробляються Правлінням Організації.
4.2. Для загального ознайомлення Політика та протоколи безпеки Організації розміщуються на сайті Організації або у друкованому вигляді у безпосередніх місцях використання.
4.3. Кожна учасниця, персонал, залучені консультантки та фахівчині, представниці, волонтерки/и, клієнтки, партнери несуть особисту відповідальність за дотримання цієї Політики та всіх протоколів та інструкцій з безпеки.
4.4. Керівництво Організації несе загальну відповідальність за створення безпечних умов праці та надання необхідних ресурсів для забезпечення безпеки. Керівництво Організації несе відповідальність за впровадження та контроль виконання Політики. Призначає відповідальну особу з питання безпеки.
4.5. Відповідальна особа за безпеку призначається наказом керівника організації. Відповідальна особа:

- Розробляє та оновлює безпекові протоколи та інструкції.
- Організовує навчання та інструктажі з питань безпеки.
- Проводить моніторинг безпекової ситуації та інформування керівництва.

- Підтримує зв’язки з відповідними органами та іншими організаціями з питань безпеки.

4.6. Керівниці проектів несуть відповідальність за ознайомлення всіх учасниць проекту із Політикою та безпековими протоколами, забезпечення безпеки персоналу проекту та клієнток під час надання послуг.

4.7. Забезпечується надійний та постійний зв'язок між усіма членкинями/ами команди та Правлінням Організації. Використовуються різні канали зв'язку:

- електронна пошта: positivewomen.ukraine@pw.org.ua
- месенджер ФБ: https://www.facebook.com/PositiveWomenUA/?locale=uk_UA
- сайт: https://pw.org.ua/kontakti/

4.8. Всі інциденти, що стосуються безпеки, повинні бути негайно зафіксовані, про ситуацію повідомлено відповідальну особу за безпеку, яка проводить аналіз ситуації і, за потреби, повідомляє Правління Організації і вносить пропозиції про зміни у Політику та безпекові протоколи для запобігання їх повторення.

4.9. Організація, за можливості, забезпечує психологічну підтримку для постраждалих та свідків інцидентів.

4.10. Порушення Політики може мати дисциплінарні наслідки, аж до звільнення, припинення договірних відносин, закінчення співпраці з Організацією без права поновлення у майбутньому, а у випадку правопорушень – відповідальність згідно з чинним законодавством України.

5. Процедури та заходи безпеки.

5.1. Безпека на об'єктах.

5.1.1. Наявність плану евакуації з приміщень. Наявність запасних виходів (в т.ч. вікна).

5.1.2. Наявність вказівників та адреси найближчого укриття.

5.1.3. Наявність маркування — знаків безпеки, інформаційних щитів та безпекових маркерів (позначки “ВИХІД”, позначення місць розміщення аптечок, вогнегасників, запасних виходів, ліхтариків, павербанків, води тощо).

5.1.4. Дотримання режиму доступу до приміщень.

5.1.5. Регулярний огляд об'єктів на предмет підозрілих предметів.

5.1.6. Наявність протипожежної сигналізації або інших протипожежних засобів, системи оповіщення, охорони.

5.1.7. Наявність необхідних запасів (вода, засоби гігієни, аптечка).

5.2. Безпека учасниць, персоналу, залучених консультанток та фахівчинь представниць, волонтерок/ів, клієнток:

5.2.1. Проведення тренінгів, навчання з безпеки (мінної безпеки, надання першої домедичної допомоги, поведінки під час обстрілів та повітряних тривог, правил поводження на блокпостах тощо).

5.2.2. Психологічна підтримка. Пошук можливостей для забезпечення доступу до психологічної підтримки для учасниць, персоналу, залучених консультанток та

фахівчинь, представниць, волонтерок/ів, клієнток, які працюють/перебувають в умовах підвищеного стресу.

5.2.3. Страхування: Пошук можливостей для страхування життя та здоров'я учасниць, персоналу, залучених консультанток та фахівчинь, представниць, волонтерок.

5.2.4. Інформаційна безпека. Захист конфіденційної інформації (дані про особу) від несанкціонованого доступу та витоку. Використання захищених каналів зв'язку. Регулярне резервне копіювання даних. Навчання правилам інформаційної гігієни та кібербезпеки.

5.2.5. Комунікаційна безпека. Обмеження обговорення оперативних планів, заходів, зібрань Організації та їх місце проведення в публічних місцях або відкритих каналах зв'язку.

6. Взаємодія з військовими, працівниками служб екстреного реагування.

6.1. Дотримання вимог та інструкцій військових та працівників служб екстреного реагування.

6.2. Забезпечення належної ідентифікації учасниць, персоналу, залучених консультанток та фахівчинь , представниць, волонтерок/ами , офісів, транспорту, майна Організації (посвідчення, бейджі, договори, наліпки, брендування та інш.)

6.3. Дотримання правил поведінки під час перевірок, на блокпостах тощо.

7. Реагування на інциденти та надзвичайні ситуації.

7.1. Розробка, дотримання протоколів реагування на різні типи надзвичайних ситуацій.

7.1.1. Протокол безпеки під час сигналу “Повітряна тривога”(Додаток 1).

7.1.2. Протокол безпеки під час зникнення мобільного зв'язку (Додаток 2).

7.1.3. Протокол безпеки під час пожежі (Додаток 3).

7.1.4. Протокол безпеки під час розширення масштабів наземних операцій, наближення зони бойових дій до місцезнаходження Організації (Додаток 4).

7.1.5. Протокол безпеки під час кібератаки (Додаток 5).

7.1.6. Комплексний протокол безпеки для учасниць заходів (Додаток 6).

8. Перегляд та оновлення Політики.

8.1. Ця Політика підлягає регулярному перегляду та оновленню (щонайменше раз на 12 місяців або у разі суттєвих змін у безпековій обстановці під час воєнного стану) з метою забезпечення її актуальності та ефективності.

8.2. Пропозиції щодо змін та доповнень до Політики можуть вноситися будь-якою учасницею, персоналом, залученою консультанткою та фахівчинею, представницею, волонтеркою/ом Організації.

8.3. Зворотній зв’язок та пропозиції щодо внесення змін до Політики та протоколів направляються відповідальній особі за безпеку на електронну пошту positivewomen.ukraine@pw.org.ua

8.4. Політика є документом, який має адаптуватися до постійно мінливих умов. Регулярні навчання, оновлення інформації та відкрита комунікація є ключовими для ефективної реалізації цієї Політики.

Протокол безпеки під час сигналу “Повітряна тривога”

Цей протокол описує дії, які необхідно здійснити у разі сигналу «Повітряна тривога» (безперервні сирени), що є попередженням про загрозу ракетного обстрілу або нальоту авіації, що дублюється на радіо й телебаченні, в соціальних мережах офіційних органів, спеціальних мобільних застосунках, таких як "Повітряна тривога" або "єТривога". Він означає, що треба негайно переміститися в захисні споруди (сховища, споруди подвійного призначення та найпростіші укриття, швидкоспоруджувані захисні споруди), які є основним засобом колективного захисту населення, або в умовно безпечні місця в будівлі (див. п.4.1. Протоколу)

1. Терміново прямувати (евакуюватися) в укриття, користуючись Планом евакуації та вказівниками про адресу, відстань та розміщення найближчого укриття.
2. Під час евакуації не користуватися ліфтами, спускатися сходами.
3. За необхідності надати допомогу тим, хто її потребує.
4. Якщо евакуація до укриття неможлива, то скористайтеся тимчасовим укриттям.
   4.1. Критерії для вибору місць тимчасового укриття в умовах відсутності захисних споруд:
   - Виконання правила «Двох (опорних, несучих) стін» та «Двох виходів».
   - Ховатися подалі від вікон та міжкімнатних дверей зі скляними елементами.
   - Використовувати сходові марші (прогони між поверхами) лише у будинках, побудованих монолітно-бетонним способом.
   - Найбільш вразливими є зовнішні приміщення, які розташовані по кутах споруд, а найбільш небезпечними поверхами — нижні (у разі вуличних боїв) та верхні (у разі авіаударів та бомбардувань).
   - Виконання формули: «3 хвилини без повітря, 3 дні без води, 3 тижні без їжі». При виборі тимчасового укриття потурбуйтесь про наявність джерел свіжого повітря (автономних систем постачання та кондиціювання повітря, що забезпечують постійний повітрообмін), запасів питної води та провізії довготривалого зберігання і без потреби приготування.
5. Перебувати в укриттях потрібно до сигналу «Відбій», про який також сповіщають сирени, радіо та телебачення або спеціальні мобільні застосунки.

Протокол безпеки на випадок зникнення мобільного зв'язку

Цей протокол описує дії, які необхідно здійснити у разі зникнення мобільного зв'язку або втрати часткової комунікації в роботі Організації для її відновлення.

1. Проведення підготовки та пошуки доступних альтернатив.

1.1. Засоби зв'язку:

- наявність повністю заряджених павербанків для телефонів.

1.2. Інформаційні джерела:

- Паперові карти місцевості, щоб орієнтуватися без доступу до GPS.
- Список важливих номерів телефонів (екстрених служб, керівниць Організації) на папері. Наприклад:

Управління пожежної охорони Києва	101
Поліція	102
Швидка медична допомога	103
Служба аварійних робіт газової мережі міста	104

1.3. Кожній членкині команди індивідуально, докласти зусиль, аби знайти джерела зв’язку (пункти незламності https://nezlamnist.gov.ua/, коворкінги.

1.5. Підготувати список членкинь команди із альтернативними контактами (з дозволу людини).

1.6. Проектні менеджерки мають підготувати письмовий перелік екстрених контактів донорів та партнерів (дану інформацію варто мати на випадок довготривалих блекаутів, коли є потреба попередження партнерів/донорів про відтермінування зустрічей, подій, подачу екстреної звітності та іншого).

1.7. Кожній членкині команди індивідуально проговорити з безпосередньою керівницею прогнозовані алгоритми своїх дій у разі втрати зв’язку на 2-3 доби.

2. Дії під час зникнення зв'язку.

2.1. Економія заряду батареї телефону:

- Вимкнути Wi-Fi, Bluetooth, GPS, мобільні дані.
- Перевести телефон у режим "У літаку".
- Зменшити яскравість екрану.

2.2. Пошук альтернативних засобів зв'язку:

Використовувати пошук мережі вручну в налаштуваннях телефону, щоб знайти доступні мережі, підключитися до внутрішнього роумінгу.

Для цього потрібно:

Відключити в телефоні автовибір мережі:

- *Для Android:* налаштування – мобільна мережа (підключення) – оператор.
- *Для iOS:* параметри – стільникові дані – вибір мережі.
- Знайти і вибрати доступну мережу вручну: *Vodafone UA, UA-KYIVSTAR* або *LIFECELL.*
- Якщо зареєструватися не вдалося, треба спробувати ще раз або вибрати іншу мережу.
- Перевірити можливість проходження дзвінка, СМС

2.3. Отримання інформації:

- Увімкнути радіоприймач на батарейках, щоб отримувати офіційні оголошення.
- Зверніть увагу на інформаційні табло, встановлені у місті, та оголошення через гучномовці.

2.4. Пересування:

- Якщо вам потрібно кудись дістатися, використовуйте паперові карти та уникайте небезпечних районів.
- Повідомте колег (якщо є можливість) про свій маршрут та орієнтовний час прибуття.

2.5. Комунікація:

- Рухайтеся до заздалегідь визначеного місця зустрічі в Організації, команді проекту, тощо.
- Залишайте повідомлення (наприклад, записки на дверях) для колег, якщо ви покидаєте офіс, вказуючи, куди ви прямуєте та коли плануєте повернутися.

3. Після відновлення зв'язку.

- Зв'яжіться з колегами. Повідомте їм про своє місцезнаходження та стан.
- Отримайте оновлену інформацію. Дізнайтеся про ситуацію в країні/регіоні/Організації та рекомендації.

Протокол безпеки під час пожежі

Цей Протокол є документом, який є життєво необхідним інструментом для ефективної організації дій, мінімізації ризиків та запобігання паніці під час пожежі та сприяє профілактиці пожеж.

1. Загальні положення та превентивні заходи:

- Наявність у кожному офісі (шелтері, пункті надання послуг) планів евакуації. Плани евакуації мають бути розміщені на видних місцях на кожному поверсі.
- Наявність вогнегасників/пожежних щитів чи протипожежної сигналізації. Розміщення вогнегасників, пожежних рукавів та іншого протипожежного обладнання промарковане, позначене.
- Наявність членкинь команди, які пройшли навчання з протипожежної безпеки та користування протипожежними засобами.
- Регулярний моніторинг вимикання електроприладів після закінчення робочого дня.
- Забезпечення вільних проходів, евакуаційних виходів та доступу до пожежного обладнання.
- Регулярне проходження інструктажів та навчання з пожежної безпеки.

2. Дії під час виявлення пожежі.

2.1. Оцінити ситуацію:

- Якщо пожежа невелика і можна її загасити, то використовуйте найближчий вогнегасник. Переконайтеся, що вихід за вашою спиною вільний.
- Якщо пожежа велика, швидко поширюється або ви не можете її загасити - негайно переходьте до евакуації.

2.2. Активуйте пожежну сигналізацію:

Натисніть кнопку ручного пожежного сповіщувача, щоб увімкнути загальну сигналізацію та сповістити всіх про небезпеку.

2.3. Повідомте екстрені служби: Якщо можливо, **зателефонуйте 101** та чітко повідомте адресу, поверх та характер події. Повідомте про пожежу іншим, щоб вони також могли вжити заходів.

3. Дії під час евакуації.

- Дотримуйтесь плану евакуації. Рухайтеся до найближчого безпечного пожежного виходу. Не користуйтеся ліфтами – вони можуть зупинитися або стати пасткою.

- Допоможіть людям з інвалідністю та обмеженими можливостями, вагітним жінкам та тим, хто потребує допомоги.
- Не забирайте особисті речі. Ваше життя та безпека важливіші за будь-які речі.
- Пересувайтеся, пригинаючись до підлоги, оскільки дим і токсичні гази піднімаються вгору. Прикривайте ніс і рот вологою тканиною, якщо це можливо.
- Закривайте двері за собою. Це допоможе стримати поширення вогню та диму.
- Після виходу з будівлі прямуйте до заздалегідь визначеного місця збору.
- Ні в якому разі не повертайтеся в охоплену вогнем будівлю, доки пожежники не дають дозволу.

4. Дії після евакуації.

- Дочекайтеся перевірки присутності всіх відповідальною особою.
- Виконуйте всі вказівки пожежників та рятувальників.
- Тримайтеся на безпечній відстані від будівлі, щоб не заважати роботі екстрених служб.
- Якщо ви відчуваєте стрес або шок, не соромтеся звернутися по допомогу до колег або спеціалістів.

Додаток №4 до Політики безпеки благодійної організації
«Позитивні жінки» в умовах воєнного стану

Протокол безпеки під час розширення масштабів наземних операцій, наближення зони бойових дій до місцезнаходження Організації

Цей Протокол є комплексним набором заходів, розроблених для забезпечення безпеки, безперервності діяльності та мінімізації ризиків для людського ресурсу, майна та репутації Організації в умовах підвищеної загрози.

1. **Безпека команди під час розширення масштабів наземних операцій, наближення зони бойових дій до місцезнаходження Організації.**

Номер пп	ПІБ	телефон	Резервний телефон(за наявності)	Адреса проживання	Адреса можливої евакуації	Контакти співмешканців (за згодою)	Контакти родичів, друзів (за згодою)	Пункт незламності, потенційного перебування

1.1. Формування контактної бази команди.
1.2. При відсутності зв'язку із членкинею команди: вивчення ситуації, комунікація за даними в таблиці, повідомлення Голові Правління.
1.3. Рекомендація членкиням команди підготувати в місці свого проживання радіо (батарейки), воду, продукти харчування, засоби альтернативного освітлення та евакуаційний багаж (тривожний чемоданчик з водою, їжею, павербанками, документами, білизною, ліками, грошима).
1.4. Рекомендація членкиням команди перевірити таблицю пунктів незламності в місці проживання і обрати найефективніший.
1.5. Рекомендація членкиням команди мати паперові примірники контактів Організації.
1.6. Рекомендація членкиням команди мати паперові контакти критичної інфраструктури в місці проживання.
1.7. Рекомендація членкиням команди пройти навчання з домедичної допомоги та регулярно поновлювати знання та навички.

2. **Безпека Організації під час розширення масштабів наземних операцій, наближення зони бойових дій до місцезнаходження Організації.**
2.1. Збереження максимальної кількості документів в електронному вигляді.
2.2. Переведення архівних документів в електронний формат.
2.3. Наявність гугл диск Організації з достатнім об'ємом.
2.4. Наявність хмарного сховища Організації з достатнім об'ємом.

2.5. Забезпечення доступу до офісу для евакуації (відповідальні особи: працівники, що мають ключі від офісу і проживають в пішому доступі або мають власні авто).
2.6. Забезпечення знищення або евакуацію документів, що містять персональні дані (відповідальні особи: головний бухгалтер, Фахівець з кадрів і фахівець з моніторингу та оцінки).
2.7. Забезпечення знищення або евакуацію печатки, факсиміле (відповідальні особи: Голова Правління, головний бухгалтер).
2.8. Забезпечення знищення або евакуацію установчих документів Організації, протоколів загальних зборів Організації, протоколів Правління (відповідальна особа: Голова Правління).

Протокол безпеки під час кібератаки

Цей протокол описує дії, які необхідно здійснити у разі кібератаки на цифрові ресурси Організації. Метою протоколу є мінімізація шкоди, відновлення функціонування систем та збереження довіри до Організації.

1. Виявлення та початкова реакція

1.1. Негайна ідентифікація: Щойно виявлено підозрілу активність (наприклад, несанкціонований доступ, зміну контенту, розсилку спаму, відмову в обслуговуванні), необхідно негайно зафіксувати час і характер події.

1.2. Ізоляція: Негайно ізолювати скомпрометовану систему від мережі (фізичне відключення мережевого кабелю або відключення Wi-Fi), за винятком випадків, коли це може призвести до незворотної втрати критичних даних або доказів атаки. У такому разі негайно зв'язатися з відповідальним за ІТ-безпеку для отримання інструкцій. Це може включати:

- Відключення сайту або переведення його в режим "технічного обслуговування";
- Зміна паролів до скомпрометованих акаунтів у соціальних мережах та месенджерах.

1.3. Повідомлення ключових осіб: Негайно повідомити керівництво Організації, відповідальну особу за безпеку, за ІТ-безпеку, та/або зовнішнього ІТ-спеціаліста.

2. Оцінка шкоди та збір доказів

2.1. Документування: Ретельно задокументувати всі відомості про атаку:

- Тип атаки (DDoS, фішинг, зламаний обліковий запис тощо);
- Час початку та виявлення;
- Які системи або дані були скомпрометовані;
- Скріншоти, лог-файли, повідомлення про помилки.

2.2. Оцінка впливу: Визначити потенційний вплив на діяльність Організації, включаючи:

- Втрату довіри з боку донорів та бенефіціарів;
- Фінансові втрати;
- Втрату або пошкодження даних.

2.3. Оцінка шкоди: Оцінка відповідності законодавству про захист персональних даних (Закон України "Про захист персональних даних").

2.4. Збереження доказів: Не видаляти та не змінювати будь-які файли або записи, які можуть бути доказами кібератаки. Це важливо для подальшого аналізу та, можливо, для правоохоронних органів.
2.5. Ланцюжок зберігання доказів: Створюючи копії лог-файлів, образів дисків чи інших доказів, необхідно задокументувати:
1) хто зробив копію,
2) коли (точна дата і час),
3) з якого джерела,
4) куди була збережена копія,
5) хеш-суми (наприклад, SHA-256) оригіналу та копії для підтвердження їх ідентичності.

3. Відновлення та реагування

3.1. Сайт:

- Відновлення з резервної копії: Якщо сайт скомпрометовано, відновити його з найсвіжішої, резервної копії. Перед відновленням сайту з резервної копії, необхідно переконатися, що сама резервна копія є "чистою" та не містить шкідливого коду. Проскануйте бекап антивірусним ПЗ у безпечному, ізольованому середовищі.
- Сканування на вразливості: Провести повне сканування сайту на наявність шкідливого програмного забезпечення та вразливостей.
- Оновлення: Переконатися, що всі плагіни, теми та CMS (система управління контентом) оновлені до останніх версій.
- Посилення безпеки: Запровадити додаткові заходи безпеки, такі як WAF (Web Application Firewall), двофакторна аутентифікація для адміністраторів, регулярне сканування на вразливості.

3.2. Соціальні мережі та месенджери:

- Зміна паролів: Негайно змінити паролі до всіх скомпрометованих акаунтів. Використовувати надійні, унікальні паролі.
- Перевірка та примусове відновлення 2FA: Негайно перевірити статус 2FA на всіх скомпрометованих та пов'язаних з ними акаунтах. Якщо вона була вимкнена зловмисником, примусово увімкнути її. Скасувати всі попередні сесії та довірені пристрої.
- Видалення шкідливого контенту: Видалити будь-який несанкціонований контент, розміщений зловмисниками.
- Повідомлення про інцидент: Повідомити підтримку соціальних мереж та месенджерів про зламаний акаунт.
- Моніторинг: Посилити моніторинг активності на цих платформах.

4. Комунікація

4.1. Внутрішня комунікація: Інформувати співробітників про інцидент, надаючи чіткі інструкції щодо подальших дій.

4.2. Зовнішня комунікація:

- Підготовка заяви: Підготувати офіційну заяву для громадськості, донорів та бенефіціарів. Заява повинна бути прозорою, але не розкривати чутливих деталей, які можуть бути використані проти організації.
- Канали комунікації: Використовувати надійні канали для поширення заяви (наприклад, офіційний прес-реліз, розсилка електронних листів, якщо вони не скомпрометовані, або інша, безпечна сторінка на сайті).
- Зберігання довіри: Запевнити громадськість у тому, що організація вживає всіх необхідних заходів для усунення наслідків та посилення безпеки.

5. Аналіз та запобігання

- Аналіз першопричин: Після усунення наслідків атаки, провести ретельний аналіз, щоб виявити першопричину інциденту та визначити слабкі місця в системі безпеки.
- Оновлення протоколів: Оновити цей протокол безпеки з урахуванням отриманого досвіду.
- Навчання персоналу: Провести додаткові тренінги для співробітників щодо основ кібербезпеки, фішингу, створення надійних паролів та важливості 2FA.
- Регулярний аудит: Впровадити регулярні аудити безпеки всіх цифрових ресурсів.
- Резервне копіювання: Забезпечити регулярне та надійне резервне копіювання всіх даних, що зберігаються як на сайті, так і в інших системах. Зберігати резервні копії на окремих, захищених носіях.

Комплексний протокол безпеки для учасниць публічних подій та заходів

Шановні учасниці заходів та колежанки!

Триваюча війна в Україні, вимагає посилення турботи про безпеку нашої роботи та волонтерства. Враховуючи активні воєнні дії росії на території України з 20 лютого 2014 року, було розроблено безпекові поради для зниження ризиків небезпеки для учасників заходів. Він є рекомендованим алгоритмом.

БО “Позитивні жінки” не несуть відповідальності за можливі наслідки воєнної агресії росії проти України, які можуть мати місце під час проведення публічних подій та заходів. Водночас, Організація докладає максимум зусиль для забезпечення безпеки членкинь своєї команди, а також учасниць та гостей наших заходів. З цією метою ми обираємо місця, які знаходяться в умовно безпечних частинах України та облаштовані укриттями або мають швидкий доступ до них.

Щиро рекомендуємо вам подбати про наступне:

1. Готуючись до участі в заході Організації самостійно та ретельно проводити безпековий аналіз населеного пункту та маршрутів до нього.
   Аналіз включає:
   - перевірку регіону на віддаленість від зони бойових дій;
   - визначення тривалості комендантської години;
   - розклад руху міського транспорту;
   - аналіз розташування захисних споруд цивільного захисту та інше.
2. У випадку пересування зонами підвищеного ризику проводити подібний посилений безпековий аналіз маршруту.
3. Визначити особу, колежанку, хто буде на зв'язку з вами, поки ви у подорожі, і попередити її про ваше планове місцезнаходження.
4. Не розкривати будь-яку інформацію, пов'язану з вашою поїздкою прямо чи опосередковано, про маршрут третім стороннім особам, які не мають відношення до маршруту та події та не є вашими близькими, родичами.
5. Пересуватися територією України з оригіналами документів, що посвідчують особу.
6. Планувати маршрут територією України з урахуванням режиму дії комендантської години, за її наявності.
7. Повідомляти організаторок про виникнення та вирішення безпекових проблем під час вашої участі у події, якщо такі проблеми виникли.
8. Плануючи поїздку, перевіряти всі документи, що посвідчують вашу особу на дійсність (термін дії, фото за віком, тощо).
9. Перевірити наявність в своєму смартфону застосунку Дія і доступ до нього.

10. Попередньо зберегти інформацію, яка містить адресу та контакти про місце поселення, бронювання тощо.
11. Мати заряджений павербанк об'ємом не менш 10000mAh, ліхтарик, аптечку та інші речі за вашою потребою.
12. ВАЖЛИВО! Одяг цивільних громадян НЕ повинен мати будь-які мілітаризовані елементи (з 24.02.2022 на території України).
13. Не залишати свій багаж з цінними речами без нагляду, або під наглядом сторонніх осіб.
14. Якщо разом з вами подорожують діти, ретельно та самостійно подбайте про їхню безпеку, наявність у вас необхідних медичних препаратів, за потреби оформити окреме медичне страхування, та попередити організаторок. Організаторки заходів не несуть відповідальності за життя та здоров'я ваших дітей під час заходів.
15. Рекомендуємо за можливості та бажання самостійно подбати про своє медичне страхування, дійсне як на території країни на весь час подорожі.
16. Уникати конфліктних ситуацій з особами, які їх провокують. Докласти максимум зусиль для уникнення конфлікту. У разі неможливості уникнути конфлікту, - за можливості викликати поліцію, вести зйомку конфлікту на свій гаджет, привернути до себе увагу колег, перехожих тощо.
17. Під час поселення в готель самостійно ознайомитися з планом евакуації.
18. Самостійно з'ясувати в місці перебування розташування укриття/бомбосховища/метро тощо.