ЗАТВЕРДЖЕНО
Наказом Президента
Благодійної організації
«Я ДОПОМОЖУ»
від 18 квітня 2025 року №32/2025
Олександр ЗЛАТІН

ПОЛІТИКА
запобігання та протидії терористичним загрозам, забезпечення безпеки, евакуації та кібербезпеки у Благодійній організації «Я ДОПОМОЖУ»
(Антитерористична політика)

1. ЗАГАЛЬНІ ПОЛОЖЕННЯ

1.1. Ця Політика запобігання та протидії терористичним загрозам, забезпечення безпеки, евакуації та кібербезпеки (далі - Політика) у Благодійній організації «Я ДОПОМОЖУ» (далі - Організація) визначає принципи, правила та процедури запобігання і реагування на загрози безпеці, організації евакуації, захисту працівників, волонтерів, бенефіціарів та майна Організації, а також забезпечення кібербезпеки та захисту інформації.

1.2. Політика є внутрішнім нормативним документом Організації та є обов'язковою для працівників, членів органів управління, волонтерів, залучених спеціалістів, підрядників, партнерів та інших осіб, які беруть участь у діяльності Організації або діють від її імені.

1.3. Політика розроблена відповідно до:

- Конституції України;
- Кримінального кодексу України;
- Кодексу цивільного захисту України;
- Закону України «Про боротьбу з тероризмом»;
- Закону України «Про основні засади забезпечення кібербезпеки України»;
- Закону України «Про захист інформації в інформаційно-комунікаційних системах»;
- Закону України «Про критичну інфраструктуру»;
- Закону України «Про благодійну діяльність та благодійні організації»;
- міжнародних стандартів та рекомендацій у сфері безпеки, цивільного захисту та кібербезпеки, що застосовуються до діяльності Організації та не суперечать законодавству України.
- інших нормативно-правових актів України у сфері безпеки, цивільного захисту та кібербезпеки;
- Статуту Організації, інших внутрішніх документів Організації та умов договорів з донорами.

1.4. Організація дотримується принципу нульової толерантності до терористичної діяльності, насильства, умисних дій, що створюють загрозу життю та здоров'ю людей, а також до дій, спрямованих на незаконне втручання в інформаційні системи Організації.

1.5. Метою Політики є:

- запобігання та мінімізація ризиків для життя, здоров'я і безпеки людей;
- забезпечення безпечних умов діяльності працівників, волонтерів, бенефіціарів та інших осіб;

- визначення порядку дій у разі виникнення загроз та надзвичайних ситуацій;
- забезпечення організованої евакуації людей у разі необхідності;
- захист майна, документів та інших активів Організації;
- захист інформації, інформаційних систем та електронних комунікацій від кіберзагроз;
- формування культури безпеки та відповідального поводження з інформацією;
- виконання вимог законодавства України та умов договорів з донорами.

2. ВИЗНАЧЕННЯ ТЕРМІНІВ

2.1. У цій Політиці терміни вживаються у такому значенні:

Тероризм - суспільно небезпечна діяльність, визначена законодавством України, що полягає у свідомому та цілеспрямованому застосуванні насильства або погрозі його застосування з метою досягнення злочинних цілей.

Терористична загроза - наявна або потенційна небезпека вчинення терористичного акту чи інших дій терористичного характеру, що можуть створити загрозу життю, здоров'ю людей, майну або діяльності Організації.

Евакуація - організоване переміщення людей із зони небезпеки до безпечного місця відповідно до встановленого порядку.

Кібербезпека - захищеність життєво важливих інтересів людини, суспільства та держави під час використання кіберпростору, відповідно до законодавства України.

Кіберзагроза - наявні або потенційно можливі явища та чинники, що створюють небезпеку в кіберпросторі та можуть негативно впливати на кібербезпеку або кіберзахист.

Кіберзахист - сукупність організаційних, правових, технічних та інших заходів, спрямованих на запобігання кіберінцидентам, захист від кіберзагроз і кібератак та відновлення функціонування інформаційних систем.

Суб'єкт Політики - працівник, член органу управління, волонтер, залучений спеціаліст, підрядник, партнер або інша особа, на яку поширюється дія цієї Політики.

Бенефіціар - фізична особа, яка отримує або має право отримувати благодійну чи гуманітарну допомогу або інші послуги від Організації.

3. СФЕРА ЗАСТОСУВАННЯ

3.1. Політика поширюється на всіх суб'єктів Політики незалежно від посади, статусу, характеру відносин з Організацією та місця виконання обов'язків.

3.2. Політика застосовується до всіх видів діяльності Організації, у тому числі під час надання благодійної та гуманітарної допомоги, взаємодії з бенефіціарами, донорами, партнерами та органами влади, використання інформаційних систем і виконання службових чи волонтерських обов'язків.

3.3. Вимоги Політики також застосовуються до дій та поведінки суб'єктів Політики поза межами Організації, якщо такі дії можуть створити загрозу безпеці людей, майну, інформації або репутації Організації.

4. ПРИНЦИПИ

4.1. Організація та всі суб'єкти Політики керуються такими принципами:

1) пріоритет життя та здоров'я людей;
2) нульова толерантність до тероризму та його фінансування чи сприяння;
3) законність;
4) запобігання та своєчасне реагування на загрози;
5) комплексний захист фізичної та інформаційної безпеки;
6) конфіденційність інформації про загрози;

7) взаємодія з компетентними державними органами;
8) персональна відповідальність за порушення вимог безпеки;
9) прозорість та підзвітність.

5. ЗАБОРОНЕНІ ДІЇ

5.1. Суб'єктам Політики забороняється:

- вчиняти або сприяти вчиненню дій терористичного характеру;
- фінансувати, матеріально чи іншим чином сприяти терористичній діяльності;
- поширювати матеріали, що пропагують тероризм або насильство;
- приховувати відому інформацію про реальну загрозу життю та здоров'ю людей;
- перешкоджати проведенню законних заходів безпеки;
- порушувати встановлені правила доступу, евакуації та безпеки;
- використовувати інформаційні системи Організації для незаконної діяльності;
- передавати третім особам паролі, ключі доступу та іншу конфіденційну інформацію без належних повноважень;
- ігнорувати сигнали оповіщення або законні вимоги відповідальних осіб під час надзвичайної ситуації.

6. ЗАПОБІГАННЯ ТА ФІЗИЧНА БЕЗПЕКА

6.1. Організація в межах своїх повноважень забезпечує:

- оцінювання ризиків та загроз безпеці;
- контроль доступу до приміщень за потреби;
- належне зберігання майна, документів та матеріальних цінностей;
- дотримання вимог пожежної, цивільної та іншої безпеки;
- готовність до реагування на надзвичайні ситуації.

6.2. Суб'єкти Політики зобов'язані негайно повідомляти відповідальних осіб або компетентні органи про підозрілі предмети, дії чи інші обставини, які можуть становити загрозу життю, здоров'ю або безпеці.

7. ЕВАКУАЦІЯ

7.1. Організація розробляє, затверджує та регулярно оновлює плани евакуації для всіх об'єктів і приміщень, що перебувають у її користуванні.

7.2. Плани евакуації передбачають:

- чітке позначення евакуаційних шляхів, виходів і місць збору;
- призначення відповідальних за евакуацію (евакуаційних координаторів) на кожному поверсі/ділянці;
- систему оповіщення (звукову, голосову, світлову, через корпоративні канали зв'язку);
- окремі сценарії дій при різних видах загроз (вибух, захоплення заручників, пожежа, комбіновані загрози тощо).

7.3. Порядок дій при оголошенні евакуації:

1. Негайне припинення роботи.
2. Вимкнення обладнання (якщо це безпечно та не створює додаткової загрози).
3. Рух до найближчого евакуаційного виходу спокійно, без паніки.
4. Надання допомоги маломобільним особам та особам з інвалідністю.
5. Збір у визначених місцях збору та перевірка присутності.
6. Заборона повернення в будівлю до офіційного дозволу відповідальних осіб або представників ДСНС.

7.4. Тренування з евакуації проводяться не рідше одного разу на рік, а за потреби - частіше. Результати тренувань фіксуються та враховуються під час удосконалення заходів безпеки..

7.5. У місцях збору забезпечується наявність аптечок, засобів індивідуального захисту (за потреби) та засобів зв'язку. Взаємодія з ДСНС і правоохоронними органами здійснюється відповідно до планів реагування.

8. КІБЕРБЕЗПЕКА

8.1. Організація забезпечує захист інформаційних систем, мереж, баз даних, каналів зв'язку та персональних даних від несанкціонованого доступу, кібератак, витоку даних та інших кіберзагроз.

8.2. Основні заходи кібербезпеки включають:

- регулярне оновлення програмного забезпечення, використання антивірусного захисту, міжмережевих екранів та систем виявлення вторгнень;
- багаторівневу автентифікацію, контроль прав доступу та принцип мінімальних привілеїв;
- регулярне резервне копіювання критичних даних та перевірку можливості їх відновлення;
- моніторинг мережевої активності та фіксацію підозрілих подій;
- навчання персоналу з питань кібергігієни (розпізнавання фішингу, соціальної інженерії, безпечне використання паролів);
- заборону використання неавторизованого програмного забезпечення та зовнішніх носіїв без попередньої перевірки;
- розробку та впровадження планів реагування на кіберінциденти (ізоляція систем, відновлення роботи, аналіз інциденту).

8.3. Усі суб'єкти Політики зобов'язані негайно повідомляти відповідальних осіб про підозрілі електронні листи, повідомлення, спроби несанкціонованого доступу, втрату пристроїв або інші ознаки кіберзагроз.

9. ПОВІДОМЛЕННЯ ПРО ПОРУШЕННЯ ТА ЗАГРОЗИ

9.1. Кожен суб'єкт Політики, а також будь-яка інша особа (включаючи бенефіціарів) має право і зобов'язаний повідомляти про відомі йому факти або обґрунтовані підозри щодо терористичних загроз, порушень правил безпеки, кіберінцидентів чи інших порушень цієї Політики.

9.2. Повідомлення може бути подане:

- письмово безпосередньо відповідальній особі за безпеку або Президенту Організації;
- електронною поштою на офіційну адресу Організації;
- через спеціальний канал повідомлень (за наявності);
- усно або іншим способом, що забезпечує фіксацію повідомлення.

9.3. Повідомлення може бути анонімним. Анонімні повідомлення розглядаються, якщо вони містять конкретну інформацію, достатню для перевірки.

9.4. Організація гарантує захист осіб, які добросовісно повідомили про можливе порушення або загрозу. Забороняється будь-яке переслідування чи негативний вплив на таких осіб у зв'язку з повідомленням.

10. РЕАГУВАННЯ ТА РОЗСЛІДУВАННЯ

10.1. Президент Організації або уповноважена ним особа організовує перевірку повідомлення у найкоротші можливі строки з дотриманням принципів конфіденційності, неупередженості та пріоритету безпеки осіб.

10.2. Під час перевірки та реагування Організація:

- забезпечує конфіденційність інформації в обсязі, необхідному для захисту осіб та інтересів Організації;
- вживає негайних заходів для усунення або мінімізації загрози;
- за наявності підстав невідкладно повідомляє компетентні державні органи відповідно до законодавства України;
- організовує евакуацію, медичну допомогу та підтримку постраждалих.

10.3. За результатами перевірки можуть бути вжиті такі заходи:

- проведення внутрішньої службової перевірки;
- притягнення винних осіб до дисциплінарної, матеріальної чи іншої відповідальності;
- звернення до правоохоронних органів;
- розірвання трудових, цивільно-правових чи партнерських відносин з винною особою;
- удосконалення внутрішніх процедур і планів безпеки.

11. ВІДПОВІДАЛЬНІСТЬ

11.1. Особи, винні у порушенні цієї Політики, несуть відповідальність відповідно до законодавства України, Статуту Організації, трудових договорів (контрактів), цивільно-правових договорів та інших внутрішніх документів.

11.2. Залежно від характеру порушення може наставати:

- дисциплінарна відповідальність (догана, звільнення тощо);
- матеріальна (цивільно-правова) відповідальність;
- адміністративна відповідальність;
- кримінальна відповідальність (у випадках, передбачених Кримінальним кодексом України).

11.3. У випадках, що містять ознаки кримінального правопорушення, Організація зобов'язана звернутися до правоохоронних органів.

12. ОЗНАЙОМЛЕННЯ ТА НАВЧАННЯ

12.1. Усі суб'єкти Політики ознайомлюються з нею до початку виконання своїх обов'язків або у найкоротший строк після її затвердження.

12.2. Організація забезпечує періодичне інформування та навчання працівників і волонтерів з питань безпеки, евакуації, кібергігієни та порядку повідомлення про загрози.

12.3. Навчання та тренування проводяться при прийнятті на роботу, початку волонтерської діяльності та надалі - у міру необхідності, але не рідше одного разу на рік.

13. ПРИКІНЦЕВІ ПОЛОЖЕННЯ

13.1. Ця Політика набирає чинності з дня її затвердження наказом Президента Організації.

13.2. Зміни та доповнення до Політики затверджуються наказом Президента Організації.

13.3. У разі зміни законодавства України положення Політики застосовуються в частині, що не суперечить чинному законодавству, до внесення відповідних змін.

13.4. Питання, не врегульовані цією Політикою, вирішуються відповідно до законодавства України, Статуту та інших внутрішніх документів Організації.

13.5. Контроль за виконанням цієї Політики покладається на Президента Благодійної організації «Я ДОПОМОЖУ» або визначену ним відповідальну особу.