ТОВАРИСТВО З ОБМЕЖЕНОЮ ВІДПОВІДАЛЬНІСТЮ

Телерадіокомпанія «РАІ»

ЗАТВЕРДЖЕНО

«25» січня 2025 р.

Директор _____ Андрій РУСИНЯК

Політика безпеки ТРК РАІ

1. Загальні положення та фундаментальні принципи

- **Нормативний статус.** Цей документ (далі — Політика) регламентує базові засади організації комплексної фізичної, цифрової, психологічної та організаційної безпеки в діяльності медіаструктури.
- **Обов'язковість виконання.** Положення цієї Політики є чинними та обов'язковими для виконання всіма штатними та позаштатними співробітниками, які діють від імені або в інтересах редакції, незалежно від юридичної форми співпраці.
- **Безумовний пріоритет безпеки.** Життя, здоров'я та особиста безпека персоналу мають абсолютний пріоритет над будь-якими виробничими потребами, виконанням редакційних завдань, дотриманням часових регламентів (дедлайнів) чи отриманням ексклюзивного інформаційного контенту.
- **Захист від примусу.** Жоден працівник компанії не може бути примушений до виконання службових обов'язків або специфічних завдань, якщо їх реалізація створює очевидну, прогнозовану або надмірну загрозу його життю та здоров'ю.
- **Врахування воєнних ризиків.** Компанія офіційно фіксує та враховує, що професійна журналістська діяльність на території України в умовах триваючого воєнного стану пов'язана з об'єктивно підвищеним рівнем небезпеки.
- **Ключові засади функціонування системи безпеки:**
  - Абсолютна превага збереження життя і здоров'я людини;
  - Виключно добровільний характер виконання завдань в умовах підвищеного ризику;
  - Запровадження методів відповідального та превентивного управління ризиками;
  - Забезпечення взаємної професійної та психологічної підтримки всередині колективу;
  - Суворе дотримання конфіденційності персональних даних персоналу;
  - Системний моніторинг та постійне вдосконалення внутрішніх безпекових протоколів.

Івано-Франківськ: вул. Василіянок, 15
0680000198 | rai@trkrai.com
rai.ua
Бурштин: вул. Січових Стрільців, 27
reklama@rai.ua

2. Стратегічна мета впровадження Політики
Реалізація цієї Політики спрямована на досягнення таких корпоративних цілей:

- Організація та підтримання максимально безпечних умов праці;
- Превентивне зниження ризиків для життя і здоров'я колективу;
- Надійний захист інформаційних, технологічних та мережевих ресурсів компанії;
- Гарантування операційної безперервності діяльності медіаплатформи;
- Чітке регламентування порядку дій та координації у разі виникнення надзвичайних ситуацій;
- Ефективна мінімізація негативних наслідків будь-яких безпекових інцидентів;
- Диференціація та фіксація зон відповідальності керівництва й персоналу у сфері безпеки.

3. Сфера правового застосування
Дія цих регламентів поширюється на весь кадровий склад компанії без винятку. При укладенні цивільно-правових договорів чи контрактів із фрилансерами, сторонніми авторами або підрядниками, редакція зобов'язана провести їхній офіційний інструктаж та ознайомити з положеннями цієї Політики до моменту фактичного початку виконання робіт.

4. Базові принципи забезпечення безпеки та правовий захист персоналу

- **4.1. Абсолютний пріоритет життя людини.** Жоден інформаційний привід, редакційний матеріал чи ексклюзивні дані не мають вищої цінності, ніж збереження життя та здоров'я людини. Співробітник наділений беззастережним правовим правом відмовитися від виконання службового доручення, якщо, на його об'єктивну оцінку, воно несе потенційну загрозу особистій безпеці. Прийняття такого рішення не може бути підставою для накладення дисциплінарних стягнень, депреміювання чи будь-яких інших форм службового тиску.
- **4.2. Добровільність виконання завдань.** Направлення співробітників у зони підвищеного ризику, райони ведення бойових дій або на території з нестабільною безпековою ситуацією здійснюється виключно за наявності їхньої офіційної добровільної згоди.

- **4.3. Професійне управління ризиками.** Процес ухвалення безпекових рішень базується виключно на попередньому експертному аналізі ризиків. Професійна конкуренція на медіаринку чи прагнення оперативного отримання ексклюзивного контенту не є аргументами для зниження стандартів захисту персоналу.
- **4.4. Принцип взаємної відповідальності.** Кожен представник кадрового складу несе персональну відповідальність як за власну безпеку, так і за безпеку колег під час спільного виконання завдань. Співробітники зобов'язані невідкладно інформувати керівництво про будь-які нововиявлені загрози чи ризики.
- **4.5. Конфіденційність логістичних та персональних даних.** Відомості про точні маршрути пересування журналістів, місця їхнього тимчасового чи постійного проживання, особисті контактні дані та інші параметри, що можуть прямо чи опосередковано вплинути на рівень їхньої захищеності, мають статус конфіденційної службової інформації. Їхнє розголошення третім особам без крайньої виробничої або правової необхідності категорично заборонено.

5. Функціональні ролі та диференціація відповідальності

5.1. Директор

У межах своїх повноважень забезпечує стратегічне управління безпекою, а саме:

- Затверджує та вводить в дію положення цієї Політики;
- Гарантує стабільне фінансування комплексних заходів безпеки;
- Організовує закупівлю сертифікованих засобів індивідуального захисту (ЗІЗ);
- Забезпечує виділення ресурсів для регулярного навчання та підвищення безпекової кваліфікації персоналу;
- Ухвалює фінальні рішення щодо повної або часткової екстреної релокації редакції;
- Здійснює загальний нагляд за дотриманням затверджених безпекових регламентів.

5.2. Головний редактор

Здійснює безпосереднє оперативне управління та контроль за дотриманням професійних стандартів безпеки:

- Проводить попередню експертну оцінку ризиків перед видачею редакційних завдань;
- Візує та погоджує службові відрядження;
- Визначає межі безпечності при виконанні завдань творчим колективом;
- Виступає організатором профільних тренінгів та інструктажів для працівників;
- Координує процеси негайного реагування у разі виникнення надзвичайних ситуацій;
- Веде особисто або призначає уповноважену особу для адміністрування Журналу обліку безпекових інцидентів;
- Забезпечує щорічний плановий перегляд та актуалізацію положень цієї Політики.

5.3. Керівники структурних підрозділів
(За наявності відповідних штатних позицій):

- Здійснюють безпосередній лінійний контроль за безпекою підпорядкованого їм персоналу;
- Оперативно інформують вище керівництво про виявлені фактори ризику;
- Контролюють суворе дотримання вимог цієї Політики на рівні своїх підрозділів.

5.4. Обов'язки та права працівників редакції
Кожен співробітник зобов'язаний:

- Беззастережно дотримуватися затверджених вимог цієї Політики;
- Своєчасно проходити планові та позапланові інструктажі;
- Правильно використовувати надані засоби індивідуального захисту;
- Не приховувати факти та прецеденти порушення безпекових протоколів колегами чи третіми особами;
- Негайно повідомляти керівництво про будь-які безпекові інциденти;
- Забезпечувати належне збереження та цілісність довіреного редакційного обладнання;
- Суворо виконувати встановлені правила цифрової та кібербезпеки;
- Підтримувати безперервний регламентований зв'язок із редакцією під час перебування у службових відрядженнях.

Кожен співробітник має право на:

- Відмову від виконання службового завдання, якщо воно пов'язане з очевидною небезпекою для життя;
- Подання анонімного повідомлення про наявні безпекові ризики чи порушення в компанії;
- Отримання професійної психологічної допомоги та реабілітації за рахунок компанії;
- Отримання вичерпної консультаційної підтримки щодо методів безпечного виконання покладених обов'язків.

6. Регламент проведення попередньої оцінки ризиків

Перед видачею та стартом будь-якого службового доручення керівництво редакції здійснює обов'язкову експертну оцінку потенційних загроз.

- **Тригери обов'язкового оцінювання.** Процедура є невід'ємною частиною планування у разі:
  - Організації службових відряджень;
  - Виконання обов'язків у прифронтових громадах та зонах підвищеної небезпеки;
  - Висвітлення масових, протестних чи суспільно-політичних заходів;
  - Роботи безпосередньо на місцях ліквідації наслідків обстрілів та ракетних ударів;
  - Здійснення професійної діяльності на деокупованих територіях;
  - Ведення складних журналістських розслідувань;
  - Реалізації інших специфічних завдань, пов'язаних із загрозою для персоналу.
- **Параметри моніторингу та аналізу.** Під час оцінювання комплексно аналізуються такі чинники:
  - Поточна військово-стратегічна та тактична ситуація;
  - Криміногенна обстановка в регіоні призначення;
  - Метеорологічні (погодні) умови;
  - Логістична та транспортна доступність локації;
  - Наявність та стан інфраструктури колективного захисту (укриттів);
  - Доступність екстреної медичної допомоги та профільних закладів охорони здоров'я;
  - Можливість реалізації планів оперативної евакуації;
  - Поточний стан фізичного та психологічного здоров'я працівника;

- Наявність та справність сертифікованих засобів індивідуального захисту (ЗІЗ);
- Надійність та дублювання каналів зв'язку;
- Забезпечення укомплектованими аптечками індивідуальної домедичної допомоги.

За результатами аналізу головний редактор або уповноважена особа з безпеки ухвалює одне з таких рішень:

1. **Санкціонувати** виконання завдання в повному обсязі;
2. **Дозволити** реалізацію за умови впровадження додаткових превентивних заходів безпеки;
3. **Пролонгувати (перенести)** терміни виконання до стабілізації обстановки;
4. **Анулювати (скасувати)** службове завдання як таке, що загрожує життю.

Шаблон фіксації даних наведений у затвердженому Додатку 1 до цієї Політики.

7. Протокол забезпечення фізичної безпеки персоналу

7.1. Матеріально-технічне забезпечення та індивідуальний захист

З метою мінімізації професійних ризиків компанія, за наявності технічної та фінансової можливості, забезпечує відряджених працівників таким інвентарем:

- Бронежилети відповідного (нормативно встановленого) класу захисту;
- Балістичні захисні каски (шоломи);
- Укомплектовані аптечки індивідуальної домедичної допомоги (стандарту IFAK);
- Світловідбивні жилети з маркуванням (за потреби);
- Автономні джерела світла (ліхтарі);
- Портативні зарядні пристрої (павербанки) та автономні зарядні станції;
- Надійні засоби телекомунікаційного зв'язку.

Працівники несуть персональну відповідальність за перевірку технічної справності, цілісності та комплектації довіреного спорядження до моменту виїзду на локацію.

7.2. Регламент дій на місцях надзвичайних подій та катастроф

Під час фіксації та висвітлення наслідків воєнних дій, обстрілів, пожеж, техногенних аварій або руйнувань журналісти зобов'язані:

- Беззастережно виконувати законні вимоги, розпорядження та рекомендації представників ДСНС, Національної поліції України, Збройних Сил України та інших уповноважених державних служб;
- Категорично уникати проникнення в аварійні, нестабільні або заміновані будівлі без офіційного супроводу чи дозволу відповідальних відомств;
- Не здійснювати діяльність у безпосередній близькості до аварійних конструкцій;
- Дотримуватися безпечної дистанції та правил роззосередження у місцях можливого повторного нанесення ударів (тактика "double tap");
- Суворо виконувати вимоги мінної безпеки;
- Постійно використовувати надані ЗІЗ відповідно до оперативної обстановки.

Редакція офіційно заявляє про неприпустимість видачі або виконання завдань, що передбачають свідоме чи навмисне ігнорування правил безпеки.

7.3. Протокол мінної безпеки
Співробітникам компанії суворо забороняється:

- Входити або в'їжджати на території, демарковані як неперевірені або нерозміновані уповноваженими службами;
- Наближатися, торкатися чи здійснювати будь-які маніпуляції з невідомими, підозрілими або потенційно вибухонебезпечними предметами;
- Самостійно пересувати залишки зброї чи техніки;
- Відхилятися від узгоджених безпечних (асфальтованих або перевірених) маршрутів пересування.

У разі візуального чи інструментального виявлення підозрілого предмета працівник зобов'язаний діяти за такою схемою:

1. **Негайно припинити рух** та зафіксувати власне положення;
2. **Організувати відхід** на безпечну відстань виключно за маршрутом попереднього заходу («слід у слід»);
3. **Оперативно здійснити виклик** екстрених служб (ДСНС за номером 101 або Поліції за номером 102);
4. **Невідкладно поінформувати** відповідальних осіб редакції про інцидент.

8. Регламент дій під час повітряної тривоги та ракетної небезпеки

- **8.1. Базовий імператив.** Збереження життя та здоров'я персоналу має абсолютну превагу над будь-якими виробничими процесами. Жодне службове доручення, збір інформації чи підготовка екстреного матеріалу не є підставою для ігнорування сигналів цивільного захисту.
- **8.2. Операційний алгоритм для персоналу.** Після активації сигналу «Повітряна тривога» кожен співробітник зобов'язаний:
  - Негайно припинити поточну діяльність у безпечний спосіб;
  - Оперативно переміститься до найближчого сертифікованого сховища чи укриття;
  - За першої технічної можливості поінформувати відповідального редактора про своє точне місцезнаходження;
  - Перебувати в захисній споруді до офіційного відбою загрози або до повної стабілізації безпекової обстановки.
- **8.3. Протокол для журналістів на місці подій.** У разі оголошення тривоги під час виконання зйомки чи репортажу, коли негайна евакуація до стаціонарного укриття є неможливою, журналіст зобов'язаний:
  - Зайняти максимально захищену точку (керуючись правилом «двох стін» або природними рельєфними укриттями);
  - Дистанційно повідомити керівництво про поточні обставини;
  - Негайно припинити фіксацію подій (фото-, відеозйомку), якщо продовження роботи збільшує ризик для життя.
- **8.4. Антикризові повноваження керівництва.** Під час інтенсивних або масованих повітряних атак головний редактор наділений повноваженнями:
  - Тимчасово зупинити операційну діяльність медіаагентства;
  - Пролонгувати часові регламенти (дедлайни) для всіх поточних матеріалів;
  - Скасувати чи відкликати раніше погоджені службові відрядження та поточні завдання.
- **8.5. Процедура звітності після відбою.** Після деактивації сигналу тривоги співробітники зобов'язані невідкладно вийти на зв'язок із керівником підрозділу та доповісти про:
  - Свій фізичний та психологічний стан;
  - Готовність до відновлення виконання посадових обов'язків;
  - Факти пошкодження або втрати службової техніки та майна;
  - Інші наслідки чи руйнування у зоні свого перебування.

9. Протокол забезпечення безперервності діяльності в умовах блекаутів
З метою мінімізації ризиків тривалих обмежень енергопостачання та втрати телекомунікаційного зв'язку, компанія впроваджує такі превентивні заходи:

- Чітке визначення та пріоритезація критично важливих редакційних процесів;
- Системне автоматичне та хмарне резервне копіювання всіх робочих матеріалів;
- Технічна та організаційна підтримка дистанційного (віддаленого) формату роботи;
- Диверсифікація каналів доступу до мережі Інтернет (використання супутникових систем, альтернативних провайдерів);
- Застосування та обслуговування автономних джерел генерації електроенергії.

Обов'язки працівників щодо підтримання автономності:

- Постійно забезпечувати максимальний рівень заряду акумуляторів мобільних телефонів та ноутбуків;
- Регулярно проводити верифікацію справності та заряджання портативних павербанків;
- Створити та підтримувати за місцем роботи індивідуальний недоторканний запас питної води та засобів особистої першої медичної допомоги;
- Завчасно завантажувати необхідні бази даних та документи на локальні носії для можливості автономної роботи без доступу до мережі.

Регламент дій за умови повної відсутності зв'язку:

- У разі неможливості надіслати звіт у встановлений термін через збій мереж, журналіст зобов'язаний вийти на зв'язок із редактором у найкоротший строк після відновлення покриття;
- При тривалій відсутності стандартних каналів зв'язку співробітник має задіяти резервні засоби комунікації (супутниковий зв'язок, радіозв'язок або альтернативні месенджери, визначені внутрішніми інструкціями);
- Якщо зв'язок із працівником, який перебуває в зоні підвищеного ризику, відсутній понад узгоджений внутрішніми регламентами час, керівництво невідкладно активує Процедуру екстреного пошуку та встановлення місцеперебування персоналу відповідно до затвердженого алгоритму.

10. Регламент забезпечення цифрової та кібербезпеки
Компанія кваліфікує цифрову безпеку як невід'ємну та критично важливу складову загальної системи корпоративного захисту та аудиту даних.

- **10.1. Контроль доступу до редакційних та мережевих ресурсів.**
  - Допуск до внутрішніх баз даних, корпоративної пошти та систем керування контентом (CMS) здійснюється виключно через персоналізовані (індивідуальні) облікові записи співробітників.
  - Персонал зобов'язаний застосовувати складні унікальні паролі та активувати дворівневу (двофакторну) автентифікацію на всіх робочих профілях і пристроях.
  - Рекомендовано використання авторизованих менеджерів паролів для захисту облікових даних.
  - Пряма чи опосередкована передача паролів, токенів доступу або ключів третім особам суворо заборонена.
- **10.2. Стандарти експлуатації робочих пристроїв.** Співробітники зобов'язані забезпечувати належний технічний захист закріпленої за ними комп'ютерної та мобільної техніки:
  - Здійснювати регулярне та своєчасне оновлення операційних систем і прикладного програмного забезпечення (ПЗ);
  - Забезпечувати безперервне функціонування ліцензійного антивірусного захисту;
  - Застосовувати автоматичне або ручне блокування екранів пристроїв у разі тимчасового залишення робочого місця;
  - Категорично уникати інсталяції неліцензійного (піратського) ПЗ або неавторизованих утиліт;
  - Повністю відмовитися від використання сторонніх USB-носіїв або інших накопичувачів без їхнього попереднього інструментального сканування на наявність шкідливого коду.
- **10.3. Безпека інформаційних потоків та реагування на загрози.**
  - Передача службової документації, чорнових варіантів матеріалів та внутрішнього листування стороннім особам без офіційного дозволу керівництва заборонена.
  - Для обміну медіафайлами та даними дозволено використовувати виключно погоджені корпоративні хмарні сервіси.
  - Про будь-які первинні ознаки кібератак, фішингу, несанкціонованого доступу або компрометації облікових даних співробітники зобов'язані негайно поінформувати технічний відділ та головного редактора.

- **10.4. Протокол захисту джерел інформації.** Компанія гарантує максимально можливий рівень захисту та конфіденційності інформаторів. Персональні дані, контакти, аудіозаписи розмов та інші відомості, що дозволяють ідентифікувати джерело, мають статус суворої службової таємниці. Їхнє розголошення чи передача третім особам без попередньої офіційної згоди самого джерела виключені, за винятком випадків, прямо передбачених чинним законодавством України на підставі судових рішень.

11. Безпековий протокол при організації та проведенні службових відряджень

Будь-яке службове виїзне завдання або відрядження підлягає обов'язковому попередньому погодженню та затвердженню головним редактором.

- **11.1. Превентивні заходи до моменту виїзду працівника.** Журналіст/автор зобов'язаний виконати такі підготовчі дії:
  - Пройти процедуру обов'язкового попереднього оцінювання ризиків;
  - Надати керівництву деталізований і затверджений маршрут пересування;
  - Зафіксувати розрахунковий час прибуття в пункт призначення;
  - Чітко погодити часові інтервали та графік виходу на контрольний зв'язок із редакцією;
  - Верифікувати максимальний рівень заряду акумуляторів усіх технічних засобів;
  - Перевірити комплектацію індивідуальної тактичної чи медичної аптечки;
  - Забезпечити наявність та належне збереження службових та особистих документів;
  - Передати координатору контактні дані осіб, із якими заплановано проведення зустрічей або інтерв'ю на локації.
- **Редакція, зі свого боку, забезпечує та фіксує:**
  - Резервний (альтернативний) логістичний маршрут;
  - Контакти екстрених служб, військових комендатур та правоохоронних органів у регіоні відрядження;
  - План та технічні засоби для проведення екстреної евакуації;
  - Призначення відповідального співробітника, який здійснює безперервний лінійний моніторинг зв'язку з відрядженою особою.

- **11.2. Регламент поведінки під час перебування у відрядженні.** Працівник зобов'язаний:
  - Суворо дотримуватися погодженого графіка та підтримувати регулярний зв'язок із куратором;
  - Невідкладно повідомляти про будь-які вимушені зміни траєкторії руху чи девіації маршруту;
  - Повністю уникати дій, пов'язаних із невиправданим ризиком для життя;
  - Беззастережно виконувати законні вимоги та розпорядження представників Збройних Сил України, Національної поліції та військових адміністрацій;
  - Негайно інформувати редакцію про виникнення критичних або непередбачуваних загроз.
- **11.3. Процедура звітності після завершення виїзного завдання.** Після повернення працівник:
  - Офіційно доповідає керівництву про безпечне завершення відрядження та прибуття до місця постійної дислокації;
  - Надає вичерпну інформацію про всі безпекові інциденти, що мали місце під час поїздки;
  - За потреби або за наявності нововиявлених факторів, формує короткий аналітичний звіт щодо специфіки ризиків на локації для врахування в майбутніх місіях компанії.

12. Протокол психологічної підтримки та захисту ментального здоров'я персоналу

- **12.1. Загальні положення.** Компанія офіційно визнає, що професійна журналістська діяльність, особливо в умовах триваючого воєнного стану, супроводжується ризиками виникнення хронічного стресу, професійного вигорання, синдрому вторинної травматизації та інших негативних психологічних наслідків. Редакція забезпечує створення безпечного та інклюзивного робочого середовища, в якому кожен співробітник має можливість відкрито заявляти про потребу в психологічній допомозі без ризику професійної дискримінації, упередженого ставлення чи кар'єрних обмежень.

- **12.2. Комплекс превентивних та реабілітаційних заходів.** За наявності організаційних та фінансових ресурсів компанія впроваджує такі інструменти підтримки:
  - Надання доступу до кваліфікованих індивідуальних консультацій із профільними психологами або психотерапевтами;
  - Організація спеціалізованих корпоративних тренінгів та семінарів з питань стресостійкості, емоційної самодопомоги та профілактики вигорання;
  - Стимулювання та нормативне забезпечення своєчасного використання працівниками щорічних відпусток та регламентованих періодів відпочинку;
  - Обов'язкове проведення індивідуальних дебрифінгів (підсумкових бесід) після повернення співробітників із зон підвищеного ризику або виконання складних завдань;
  - Культивація та підтримання внутрішньої етики взаємоповаги, солідарності та колегіальної підтримки всередині колективу.
- **12.3. Професійні права працівника у сфері ментального здоров'я.** Кожен співробітник наділений законним правом:
  - Подати офіційний або конфіденційний запит на отримання психологічної підтримки за рахунок компанії;
  - Своєчасно поінформувати безпосереднього керівника про виявлення первинних симптомів емоційного або професійного виснаження;
  - Реалізувати право на тимчасову відмову від виконання нових службових доручень після пережитої травматичної чи критичної події на локації до моменту повної психоемоційної реабілітації та відновлення працездатності.

13. План забезпечення операційної безперервності діяльності медіаструктури (BCP)

- **13.1. Стратегічна мета.** Головною метою цього Плану є гарантування безперебійного, стабільного та автономного функціонування всіх ключових підрозділів редакції за умов виникнення надзвичайних ситуацій, техногенних катастроф, блекаутів або безпекових криз.

13.2. Перелік критично важливих корпоративних функцій. До процесів, що підлягають першочерговому відновленню та безперервному підтриманню, належать:

- **Мовлення та новини:** безперебійний ефір радіо й телебачення, а також оперативний випуск новинної стрічки на сайті.
- **Технічна стабільність:** адміністрування, захист вебсайту та збереження доступу до цифрових медіаархівів.
- **Зв'язок:** робота офіційної пошти, каналів комунікації з **аудиторією** та внутрішнього зв'язку між працівниками.
- **Безпека даних:** регулярне резервне копіювання (бекап) критичних баз даних та систем.
- **Фінанси:** доступ до бухгалтерської, фінансової та звітної документації компанії.

- **13.3. Антикризові заходи та інструменти автоматизації.** З метою реалізації Плану компанія забезпечує:
  - Надійне автономне та резервне збереження документів суворої звітності;
  - Повний перехід на ліцензійні хмарні сервіси для організації спільної роботи;
  - Обов'язкове дублювання прав доступу (паролів, токенів, ключів) до критичних мережевих ресурсів серед обмеженого кола керівництва;
  - Впровадження системи крос-функціональної взаємозамінності (матриці компетенцій) працівників для оперативного перерозподілу обов'язків;
  - Технічну та регламентну готовність до негайного і повного переведення всієї структури на дистанційний (віддалений) формат роботи.

14. Регламент та порядок евакуації (релокації) редакції

- **14.1. Юридичні та фактичні підстави.** Рішення про повну або часткову зміну географічної дислокації та переміщення потужностей компанії ухвалюється за наявності таких критичних чинників:
  - Верещення безпосередніх або активних бойових дій у регіоні розташування офісу;
  - Систематичні ракетно-артилерійські обстріли або удари БПЛА по інфраструктурі міста;

- Фактична окупація, оточення або підтверджена загроза окупації території;
- Об'єктивна неможливість забезпечення базових безпечних умов для життєдіяльності та праці персоналу;
- Тривале та масштабне припинення постачання енергоносіїв, води або критичного зв'язку (деструкція комунальної інфраструктури);
- Інші форс-мажорні та надзвичайні обставини, що унеможливлюють операційну діяльність.

- **14.2. Процедура ухвалення рішень.** Фінальне рішення про переміщення (релокацію) ухвалює виключно Директор або засновник медіаагентства за результатами обов'язкових консультацій із головним редактором та аналітиками з безпеки.
- **14.3. Операційний алгоритм під час здійснення переміщення.** Компанія забезпечує виконання таких скоординованих дій:
  - Попередній аналіз, вибір та верифікація безпечної цільової локації для відновлення роботи;
  - Офіційне та оперативне сповіщення персоналу щодо термінів, логістики та порядку евакуації;
  - Здійснення повного екстреного резервного копіювання корпоративних баз даних та архівів на захищені віддалені сервіси;
  - Організація логістики, пакування та безпечного транспортування матеріальних активів і високотехнологічного обладнання (за наявності безпечного коридору);
  - Безперервна підтримка та організація повноцінної дистанційної роботи колективу на етапі здійснення транзиту.
- **14.4. Регламент селективної (часткової) релокації.** У разі виникнення індивідуальних загроз, компанія впроваджує процедуру точкового переміщення окремих критично важливих спеціалістів або структурних підрозділів (наприклад, серверного вузла чи стрічки новин) без обов'язкового зупинення чи переміщення стаціонарного офісу.

15. Порядок реєстрації безпекових інцидентів та ведення внутрішнього аудиту

З метою забезпечення прозорості та належного контролю, компанія впроваджує обов'язковий внутрішній Журнал реєстрації безпекових інцидентів.

- **Перелік подій, що підлягають безумовній каталографії:**
  - Виробничі, побутові чи воєнні травми, отримані персоналом під час виконання обов'язків;
  - Дорожньо-транспортні пригоди (ДТП) за участю співробітників чи службового транспорту;
  - Кібератаки, спроби фішингу, DDoS-атаки або факти компрометації мережевих ресурсів;
  - Офіційні чи анонімні погрози, тиск, переслідування журналістів з боку третіх осіб;
  - Факти навмисного чи випадкового пошкодження нерухомого майна компанії;
  - Втрата, викрадення або знищення службової техніки, зброї чи засобів індивідуального захисту;
  - Безпідставні або процесуальні затримання співробітників правоохоронними чи військовими органами;
  - Будь-які інші суттєві порушення протоколів інформаційної або фізичної безпеки.
- **Аналіз та запобігання.** За фактом фіксації кожного серйозного безпекового інциденту головний редактор скликає внутрішню комісію для детального аналізу причин події, оцінки дій персоналу та розробки обов'язкових превентивних заходів задля недопущення аналогічних кейсів у майбутньому.

16. Протокол негайного реагування на надзвичайні ситуації

У разі раптового виникнення форс-мажорних обставин чи надзвичайної події, кожен співробітник зобов'язаний суворо дотримуватися такої послідовності дій:

1. **Забезпечити особисту безпеку** (використати укриття, зупинити рух, залишити небезпечну зону);
2. **Невідкладно сповістити** відповідального координатора або керівництво редакції про свій стан та характер загрози;
3. **Здійснити екстрений виклик** державних служб порятунку (ДСНС — 101, Поліція — 102, Швидка допомога — 103) за наявності об'єктивної потреби;
4. **Беззастережно виконувати** легітимні вказівки, команди та розпорядження представників рятувальних або військових відомств на локації;
5. **Надати вичерпну інформацію** та хронологію подій керівництву після повної стабілізації ситуації та ліквідації безпосередньої загрози.

З боку компанії під час кризового інциденту забезпечується:

- Безперервний моніторинг та підтримання зв'язку з постраждалим працівником;
- Оперативна координація надання медичної, правової, логістичної чи матеріальної допомоги;
- Офіційне документування та юридична фіксація обставин події;
- Проведення комплексного розслідування безпекових чинників;
- Запровадження позапланових змін та оновлень до положень цієї Політики на основі отриманого досвіду.

17. Регламент професійного навчання та безпекової підготовки персоналу
Компанія впроваджує систему планового навчання та підвищення кваліфікації кадрового складу задля мінімізації операційних ризиків.

- **Ключові напрями освітніх програм та тренінгів:**
  - Надання невідкладної домедичної допомоги (згідно з міжнародними протоколами);
  - Дотримання вимог та правил мінної безпеки на деокупованих і прифронтових територіях;
  - Забезпечення особистої фізичної безпеки та захисту під час виконання завдань;
  - Впровадження інструментів цифрової безпеки та кібергігієни в повсякденну роботу;
  - Алгоритми дій та координація під час ліквідації наслідків надзвичайних ситуацій;
  - Методи підтримання психологічної стійкості, самодопомоги та протидії стресу;
  - Специфіка та правила здійснення професійної діяльності безпосередньо в умовах ведення бойових дій.
- **Процедура онбордингу.** Усі новоприйняті штатні працівники, а також залучені контрагенти й фрилансери підлягають обов'язковому ознайомленню з положеннями цієї Політики, проходженню первинного інструктажу та верифікації знань до моменту фактичного початку виконання своїх посадових обов'язків чи отримання першого редакційного завдання.

19. Порядок моніторингу, актуалізації та перегляду Політики
Цей документ підлягає обов'язковому плановому та позаплановому аудиту для підтримання його ефективності й відповідності оперативній обстановці.

- **Перелік обставин, що зумовлюють перегляд Політики:**
  - Плановий внутрішній аудит (проводиться регулярно, не рідше одного разу на календарний рік);
  - Виникнення та розбір серйозних безпекових інцидентів або правопорушень у компанії;
  - Внесення суттєвих змін до профільного законодавства України (зокрема медіазаконодавства чи оборонних нормативних актів);
  - Кардинальна зміна безпекової, стратегічної чи тактичної ситуації в країні або регіонах присутності видання;
  - Реалізація процедури повної або часткової релокації (евакуації) офісу та потужностей редакції;
  - Результати та приписи комплексного внутрішнього чи зовнішнього безпекового аудиту медіаструктури.
- **Юридичне затвердження змін.** Будь-які модифікації, доповнення, розширення або оновлення положень цієї Політики безпеки розробляються координаційною радою під керівництвом головного редактора та набувають чинності виключно після їхнього офіційного затвердження відповідним Наказом Директора компанії.

ДОДАТКИ ДО ПОЛІТИКИ БЕЗПЕКИ РЕДАКЦІЇ

Додаток 1. Форма обов'язкової оцінки ризиків перед службовим відрядженням

Ця форма заповнюється відповідальним координатором та затверджується керівництвом до моменту виїзду персоналу на локацію.

№ п/п	Параметр верифікації та моніторингу ризику	Так	Ні	Експертний коментар / Обґрунтування
1	Точні координати та місце призначення відрядження визначено			
2	Основний логістичний маршрут пересування погоджено			
3	Оперативний аналіз безпекової ситуації в регіоні проведено			
4	Наявність та доступність інфраструктури захисту (укриттів) перевірено			
5	Рівень загрози ракетно-артилерійських обстрілів ідентифіковано			
6	Стан мінної небезпеки та статус розмінування території верифіковано			
7	Резервний маршрут екстреної евакуації розроблено та погоджено			
8	Працівника забезпечено аптечкою індивідуальної домедичної допомоги			
9	Працівника забезпечено балістичною захисною каскою (шоломом)			
10	Працівника забезпечено бронежилетом належного класу захисту			
11	Технічний стан та готовність транспортного засобу перевірено			
12	Часові інтервали та графік контрольного виходу на зв'язок затверджено			
13	Призначено відповідальну лінійну особу з боку редакції			

Офіційне рішення керівництва за результатами оцінювання:

- [ ] **Санкціонувати** виконання службового завдання в повному обсязі.
- [ ] **Дозволити** реалізацію місії за умови впровадження додаткових превентивних заходів.
- [ ] **Пролонгувати (відкласти)** виконання завдання до стабілізації безпекової обстановки.
- [ ] **Анулювати (скасувати)** службове відрядження у зв'язку з надмірним рівнем загрози.

Додаток 2. Журнал реєстрації та внутрішнього аудиту безпекових інцидентів

Усі задекларовані прецеденти та порушення підлягають обов'язковому внесенню до цього Реєстру для формування аудиторського сліду.

Дата та час	ПІБ та посада працівника	Категорія та вид інциденту	Географічна локація	Стисла сутнісна характеристика	Впроваджені заходи реагування	ПІБ відповідальної особи	Додаткові примітки

Додаток 3. Чек-лист готовності журналіста до виїзду у службове відрядження

Обов'язковий до виконання та самоперевірки співробітником безпосередньо перед залишенням місця постійної дислокації.

- **Юридичне та службове забезпечення:**
  - [ ] Чинне редакційне (журналістське) посвідчення встановленого зразка;
  - [ ] Паспорт громадянина України або інший документ, що офіційно посвідчує особу.
- **Енергетична автономія та зв'язок:**
  - [ ] Максимальний рівень заряду акумулятора мобільного телефона;
  - [ ] Справні портативні джерела живлення (павербанки) зі 100% рівнем заряду;
  - [ ] Максимальний рівень заряду акумулятора робочого ноутбука;
  - [ ] Наявність засобів для активації резервного чи альтернативного способу зв'язку.

- **Медичний та індивідуальний захист:**
  - [ ] Повністю укомплектована медична аптечка індивідуальної домедичної допомоги (IFAK);
  - [ ] Балістична захисна каска (шолом) — *за умови підвищеного ризику*;
  - [ ] Бронежилет відповідного класу захисту з належним маркуванням — *за умови підвищеного ризику*.
- **Життєзабезпечення та логістика:**
  - [ ] Індивідуальний недоторканний запас питної води;
  - [ ] Продуктовий набір (запас їжі) тривалого зберігання;
  - [ ] Автономне джерело світла (портативний або налобний ліхтар).
- **Інформаційна координація:**
  - [ ] Актуальні прямі контакти відповідального лінійного редактора;
  - [ ] Номери телефонів екстрених та рятувальних служб у регіоні відрядження;
  - [ ] Деталізована карта затвердженого основного та резервного маршрутів пересування;
  - [ ] Перелік та точні координати верифікованих інфраструктурних укриттів на маршруті;
  - [ ] Актуальний метеорологічний прогноз та дані про погодні умови у зоні виконання завдань.

Додаток 4. Регламентований алгоритм дій у разі втрати телекомунікаційного зв'язку з журналістом

1. **Етап первинного моніторингу:** У разі відсутності виходу співробітника на контрольний зв'язок у чітко затверджений часовий інтервал, відповідальний лінійний редактор зобов'язаний негайно здійснити спроби встановлення контакту за допомогою всіх наявних основних та альтернативних каналів комунікації (телефонний зв'язок, месенджери, супутниковий зв'язок).
2. **Етап внутрішнього розшуку:** Якщо протягом **30 хвилин** із моменту пропуску контрольного часу зв'язок встановити не вдалося, відповідальний редактор здійснює екстрений виклик довіреної (контактної) особи, яку журналіст офіційно зазначив у формі перед виїздом у відрядження.

3. **Етап екстреного реагування:** У разі безперервної відсутності зв'язку з працівником, який перебуває в зоні підвищеного ризику, понад **1 (одну) годину**, головний редактор ініціює процедуру залучення державних органів. На основі аналізу останніх відомих координат здійснюється офіційне звернення до підрозділів ДСНС, Національної поліції України, військових комендатур або відповідних обласних військових адміністрацій (ОВА).
4. **Етап фіксації:** Усі впроваджені заходи, хронологія телефонних дзвінків та отримана від держорганів інформація підлягають похвилинній фіксації у Журналі реєстрації інцидентів.

Додаток 5. Стратегічний план екстреної релокації та евакуації потужностей редакції

У разі офіційного затвердження Наказу про повну або часткову зміну географічної дислокації підприємства, реалізуються такі скоординовані етапи:

1. **Управління процесом:** Негайне формування Антикризової координаційної групи під керівництвом Генерального директора та головного редактора.
2. **Захист інформаційних активів:** Здійснення екстреного повного дзеркалювання, шифрування та хмарного резервного копіювання всіх баз даних, архівів, журналістських матеріалів та фінансової звітності.
3. **Логістика матеріальних активів:** Складання пріоритетного переліку, маркування, пакування та підготовка до першочергового транспортування високотехнологічного обладнання, серверів та засобів захисту.
4. **Кадрова координація:** Проведення офіційного інструктажу персоналу, доведення до відома співробітників адреси нової безпечної локації, логістичних маршрутів та порядку компенсації витрат на переїзд.
5. **Операційна безперервність:** Забезпечення негайного та безперебійного переходу всього творчого та адміністративного колективу на віддалений (дистанційний) формат роботи з метою збереження безперервності стрічки новин на етапі транзиту.
6. **Інфраструктурний аудит:** Організація та перевірка віддалених прав доступу, захищених VPN-каналів до серверів, цифрових архівів та систем керування контентом (CMS) з нових робочих місць.
7. **Фінальна верифікація:** Проведення комплексного внутрішнього аудиту працездатності всіх критично важливих бізнес-процесів медіаагентства після завершення фізичного переміщення та розгортання потужностей на новій локації.