ОБ'ЄДНАНІ
любов'ю до дітей

ГРОМАДСЬКА ОРГАНІЗАЦІЯ «ОБ'ЄДНАНІ ЛЮБОВ'Ю ДО ДІТЕЙ»

ЄДРПОУ: 45179507
м. Херсон, Україна

ЗАТВЕРДЖЕНО
Наказом Голови Організації
№ 8 від «20» квітня 2026 року
Голова Організації

_____ /Костінюк І.В./

ПОЛІТИКА З КІБЕРБЕЗПЕКИ

Тип документа: Policy
Код документа: POL-SEC-012
Версія: 1.0
Дата затвердження: 20.04.2026
Дата набрання чинності: 20.04.2026
Дата наступного перегляду: 20.04.2027

м. Херсон, 2026 рік

МЕТА ПОЛІТИКИ: Ця політика встановлює принципи та правила забезпечення цифрової та кібербезпеки в діяльності ГО «Об'єднані любов'ю» з метою: захисту інформації, персональних даних, цифрової інфраструктури; забезпечення безперервності роботи; запобігання кібератакам, витокам інформації або внутрішнім загрозам.

Для громадської організації «Об'єднані любов'ю», яка працює з фінансами та персональними даними, політика кібербезпеки це захист від крадіжки грантових коштів та витоку даних бенефіціарів.

Ключові принципи цифрової безпеки:

Конфіденційність: захист персональних та чутливих даних.

Цілісність: недопущення несанкціонованої зміни чи знищення даних.

Доступність: своєчасний доступ до даних для уповноважених осіб.

Контроль доступу: права доступу обмежуються відповідно до ролей.

Обізнаність: регулярне навчання команди з цифрової безпеки.

Цифрові активи, які охоплює політика:

Облікові записи (ел. пошта, Google Drive, CRM, месенджери тощо)

Пристрої (ноутбуки, смартфони, зовнішні накопичувачі)

Цифрові сервіси (сховище, платформи донорів, сайти)

Бази даних (бенефіціари, партнери, внутрішні документи)

Паролі, токени, ключі доступу

1. ПАРОЛІ ТА ДОСТУПИ

1.1. Двофакторна автентифікація (2FA): Обов'язкова для всіх робочих акаунтів (Google, Microsoft, Facebook, Банкінг). Без 2FA доступ до фінансових документів заборонено.

1.2. Складність: Пароль має містити >12 символів. Заборонено використовувати імена, дати народження або назву організації.

1.3. Зберігання: Використання менеджерів паролів (напр. Bitwarden). Заборонено зберігати паролі в браузерах або на папірцях.

2. БЕЗПЕКА ФІНАНСОВИХ ОПЕРАЦІЙ

2.1. Електронний підпис (ЕЦП): Зберігається виключно на захищеному носії (токені) або у хмарному сховищі банку з паролем, відомим лише власнику ключа. Передача ключа іншим особам заборонена.

2.2. Верифікація реквізитів: При отриманні нових банківських реквізитів від постачальника електронною поштою, менеджер зобов'язаний підтвердити їх голосом по телефону (захист від підміни інвойсів).

2.3.Публічні мережі: Категорично заборонено проводити банківські операції через відкритий Wi-Fi (кафе, вокзали) без увімкненого VPN.

3. РОБОТА З ДАНИМИ ТА ХМАРОЮ

3.1. Права доступу: Доступ до папок з фінансовими звітами та персональними даними бенефіціарів надається за принципом «мінімальної необхідності».

3.2. Посилання: Заборонено створення «публічних посилань» (доступ для всіх, у кого є лінк). Доступ надається лише на конкретну електронну пошту.

3.3. Звільнення: Протягом 2 годин після звільнення працівника системний адміністратор або бухгалтер анулює всі його доступи до пошти, дисків та банків.

4. РОБОЧІ ПРИСТРОЇ

4.1. Блокування: Екран має автоматично блокуватися через 2 хвилини бездіяльності.

4.2. Антивірус: На кожному пристрої має бути встановлене ліцензійне та оновлене антивірусне ПЗ.

4.3. Шифрування: Робочі ноутбуки повинні мати активоване шифрування дисків (BitLocker/FileVault) на випадок крадіжки.

5. ПРОТОКОЛ РЕАГУВАННЯ НА ІНЦИДЕНТИ

У разі підозри на злам або втрати пристрою:

5.1. Протягом 30 хв: Повідомити керівника та бухгалтера.

5.2. Протягом 1 год: Змінити паролі до пошти та банківських систем.

5.3. Протягом 2 год: Дистанційно вийти з усіх сесій на втраченому пристрої.

5.4. Правила щодо електронного зв'язку

6. ОГЛЯД

6.1. Всі електронні та телефонні комунікації з використанням будь-яких систем, якими володіє, які ліцензує або якими управляє Організація (комунікаційні системи Організації) повинні розглядатись як такі, що знаходяться на балансі Організації, тобто як майно Організації. Якщо дозволяється тимчасове особисте користування комунікаційними системами Організації, користувачі при цьому не можуть претендувати на конфіденційність.

7. КОНФІДЕНЦІЙНА ІНФОРМАЦІЯ

7.1. Користувачі комунікаційних систем Організації повинні дотримуватися правил конфіденційності. Користувачі повинні застережливо ставитися до відправки

конфіденційної інформації через комунікаційні системи Організації, оскільки через такі системи легше зробити неправильну або неуважну розсилку, ніж через інші засоби комунікації. Конфіденційну інформацію не можна надсилати через Інтернет, якщо при цьому не користуватися механізмами шифруванням чи іншими засобами безпеки. Конфіденційну інформацію в мережі Організації потрібно забезпечувати паролем і вилучати з мережі, якщо вона непотрібна.

8. АВТОРСЬКЕ ПРАВО

8.1. Забороняється використання комунікаційних систем Організації для копіювання, модифікації або передачі документів, програмного забезпечення, інформації або інших матеріалів, захищених авторським правом, торговою маркою, патентом чи законодавством про комерційну таємницю, без погодження з власником таких прав на ці матеріали. Має використовуватись лише ліцензійне програмне забезпечення.

9. ЕТИКЕТ

9.1. Використання електронних та телефонних засобів комунікації користувачами комунікаційних систем Організації повинно мати ввічливий, професійний та діловий характер. Всі повідомлення можуть підлягати розкриттю під час розгляду судових справ або проведення інших правових процедур. Окрім того, важливо мати на увазі те, що «знищення» повідомлення на вашому комп'ютері може не означати його зникнення повністю з пам'яті комп'ютера, оскільки мережа відправника або мережа отримувача може мати систему резервної архівації.

10. ЗБЕРЕЖЕННЯ ЕЛЕКТРОННИХ ЗАПИСІВ

10.1. Користувачі комунікаційних систем Організацій повинні зберігати лише ті електронні та телефонні повідомлення, які необхідні для ведення бізнесу або виконання регулятивних чи правових вимог, і утримувати їх якомога коротший період часу - лише для досягнення бізнесових, правових або регулятивних цілей.

10.2. З метою забезпечення максимального захисту інформації від можливого ушкодження Організація повинна забезпечити зберігання резервних копій фінансової інформації. Частота зберігання резервних копій визначається частотою проведення операцій.

10.3. Користувачі комп'ютерів несуть відповідальність за безпеку файлів та програмного забезпечення, встановленого на офісних комп'ютерах.

11. ДІЇ У ВИПАДКУ ІНЦИДЕНТІВ

У разі виявлення підозрілої активності, втрати пристрою або кібератаки:

Негайно інформується відповідальна особа_____

Змінюються паролі та вживаються заходи ізоляції.

Фіксується інцидент і проводиться внутрішнє розслідування.

12. НАВЧАННЯ ТА ВІДПОВІДАЛЬНІСТЬ

Всі працівники проходять інструктаж з кібербезпеки.

Нові члени команди підписують зобов'язання дотримуватись політики. Цей документ зберігається 5 років поки працює особа і 2 після звільнення.

Порушення політики тягне за собою дисциплінарну відповідальність.

13. АКТУАЛІЗАЦІЯ ПОЛІТИКИ

Політика переглядається не рідше ніж один раз на рік або при виявленні нових ризиків.

ІНВЕНТАРНИЙ ЧЕК-ЛІСТ (ДЛЯ ІТ-АУДИТУ)

(Заповнюється раз на квартал)

Назва пристрою	Відповідальна особа	Антивірус (Так/Ні)	2FA активована	Шифрування диска
Ноутбук HP #1	Бухгалтер	Так	Так	Так
Планшет Apple	Координатор	Так	Так	Так

2. Зобов'язання про нерозголошення (NDA) та безпеку

(Підписується кожним працівником при прийомі на роботу)

Зобов'язання про конфіденційність та цифрову гігієну Я, [ПІБ], працюючи в ГО «Об'єднані любов'ю», зобов'язуюсь:

1. Не розголошувати фінансові дані організації та персональні дані бенефіціарів третім особам.

2. Використовувати двофакторну автентифікацію на всіх робочих акаунтах.

3. Негайно (протягом 30 хв) повідомляти керівництво про втрату робочого пристрою або підозру на злам пошти.

4. Не передавати свої паролі та електронні ключі (ЕЦП) іншим співробітникам.

5. Дата: _____ Підпис: _____

3. Графік регулярних перевірок (Контрольний календар)
Цей список допоможе вам підтримувати порядок без зайвих зусиль:

- Щотижня (П'ятниця): Менеджери здають чеки та акти бухгалтеру.
- Щомісяця (1-5 число): Перевірка табелів (Time-sheets) та підписання актів з експертами за минулий місяць.
- Щокварталу:
  - Аудит доступів до хмарних папок (видалення зайвих людей).
  - Зміна критичних паролів (якщо не використовується менеджер паролів).
  - Перевірка термінів дії ЕЦП та ліцензій антивірусів.

УГОДА ПРО НЕРОЗГОЛОШЕННЯ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ (NDA)

м. [Місто] ____-----«__» _____ *2026* р.

ГО «Об'єднані любов'ю» (далі — Організація), в особі Директора [ПІБ], з однієї сторони, та [ПІБ працівника/волонтера] (далі - Отримувач), з іншої сторони, уклали цю Угоду про наступне:

1. Предмет Угоди

Отримувач зобов'язується не розголошувати третім особам Конфіденційну інформацію, яка стала йому відома у зв'язку з виконанням професійних чи волонтерських обов'язків в Організації.

2. Що вважається Конфіденційною інформацією

- Фінанси: Бюджети грантів, суми гонорарів, банківські виписки, логіни/паролі до банк-клієнтів.
- Персональні дані: Списки бенефіціарів (ПІБ, телефони, адреси осіб, яким допомагає ГО).
- Цифрова безпека: Паролі до пошти, хмарних сховищ, ключі ЕЦП, налаштування серверів.
- Стратегія: Переговори з донорами, умови ще не підписаних грантових угод.

3. Зобов'язання Отримувача

- Використовувати інформацію виключно для роботи в Організації.
- Зберігати в таємниці всі паролі та коди доступу, не передавати їх стороннім особам.
- У разі звільнення - негайно видалити всі робочі файли з особистих пристроїв та повернути майно ГО.
- Термін дії: Зобов'язання діють протягом роботи в ГО та 3 роки після припинення співпраці.

4. Відповідальність

За розголошення інформації Отримувач несе відповідальність згідно з законодавством України та внутрішніми правилами Організації (включно з негайним розірванням договору та відшкодуванням збитків).

ПІДПИСИ СТОРІН:

Від Організації: _____ / [Прізвище] /

Отримувач: _____ / [Прізвище] /