

«ЗАТВЕРДЖЕНО»

в.о. Голови Правління

Сиротенко К.П.

28 січня 2025



Політика з використання інформаційно-комунікаційних технологій

1. Загальні положення

1.1. Дана політика регулює правила використання інформаційно-комунікаційних технологій (ІКТ) співробітниками, волонтерами та іншими зацікавленими сторонами, пов'язаними з діяльністю Благодійного фонду «БЛАГОМАЙ».

1.2. Мета політики – забезпечити ефективне, безпечне та етичне використання ІКТ для виконання завдань фонду.

1.3. До ІКТ належать: електронна пошта, месенджери, соціальні мережі, сайти, сервіси для управління проектами, програмне забезпечення та обладнання, що використовується в діяльності фонду.

2. Принципи використання ІКТ

2.1. Ефективність: Використання ІКТ має сприяти досягненню цілей фонду.

2.2. Безпека: Усі дані, які передаються через ІКТ, повинні захищатися від несанкціонованого доступу.

2.3. Етичність: Забороняється використання ІКТ для поширення дискримінаційної, образливої, недостовірної чи шкідливої інформації.

2.4. Дотримання законодавства: Усі дії в межах використання ІКТ мають відповідати чинному законодавству України та внутрішнім нормативним документам фонду.

3. Вимоги до користувачів ІКТ

3.1. Усі співробітники та волонтери, які отримують доступ до ІКТ фонду, зобов'язані:

- Використовувати ІКТ лише для виконання завдань фонду.
- Забезпечувати конфіденційність інформації, пов'язаної з діяльністю фонду.
- Уникати дій, що можуть загрожувати безпеці обладнання або інформації (наприклад, встановлення неавторизованих програм).
- Регулярно оновлювати паролі до облікових записів, пов'язаних із діяльністю фонду.

3.2. Забороняється:

- Використовувати технічні та інформаційні ресурси фонду для особистої вигоди.
- Поширювати інформацію, що порушує права та свободи інших осіб.

- Відкривати посилання чи вкладення в електронних листах від невідомих джерел, які можуть містити віруси чи шкідливе ПЗ.

4. Управління соціальними мережами та веб-ресурсами фонду

4.1. Доступ до облікових записів у соціальних мережах, сайтів і сервісів надається лише уповноваженим особам.

4.2. Контент, який публікується, має відповідати цінностям і місії фонду, бути достовірним і перевіреним.

4.3. Забороняється публікація персональних даних бенефіціарів без їхньої письмової згоди.

5. Обладнання та технічна підтримка

5.1. Технічне обладнання (комп'ютери, телефони, планшети) надається працівникам фонду виключно для виконання службових обов'язків.

5.2. Використання обладнання:

- Користувачі зобов'язані підтримувати технічний стан обладнання та повідомляти про несправності відповідальній особі;
- Заборонено передавати обладнання третім особам без дозволу керівництва.

5.3. Заборонено використовувати обладнання фонду для цілей, не пов'язаних із його діяльністю.

5.4. Технічне обслуговування:

- Обладнання регулярно проходить технічний огляд відповідальною особою або відділом технічної підтримки.
- Співробітники зобов'язані негайно повідомляти про несправності, збої чи пошкодження обладнання.

5.5. Програмне забезпечення:

- Встановлення нового програмного забезпечення дозволено лише за погодженням із відповідальним за технічну підтримку.
- Заборонено використовувати неліцензійне або несанкціоноване програмне забезпечення.

5.6. Видалення даних:

Перед поверненням обладнання до фонду (наприклад, після завершення контракту) користувачі повинні видалити всі персональні дані з пристроїв.

6. Політика зберігання та захисту даних

6.1. Уся інформація, яка стосується діяльності фонду, зберігається на офіційних серверах або у хмарних сервісах з високим рівнем захисту.

6.2. Дані про бенефіціарів, донорів і партнерів є конфіденційними та використовуються виключно для досягнення статутних цілей фонду. Доступ до конфіденційних даних надається лише працівникам, які мають відповідні повноваження.

6.3. У разі виявлення витоку інформації, співробітники зобов'язані негайно повідомити керівництво.

6.4. Безпека даних:

- Для захисту даних використовуються паролі, багатофакторна автентифікація та шифрування.
- Заборонено зберігати конфіденційні дані на особистих пристроях працівників.

6.5. Інциденти витоку даних:

- У разі виявлення витоку інформації співробітники зобов'язані негайно повідомити відповідальну особу або керівництво фонду.
- Проводиться розслідування причин інциденту та вживаються заходи для усунення наслідків.

7. Управління цифровими комунікаціями

7.1 Офіційні комунікації: Лише затверджені платформи та канали використовуються для офіційної комунікації з донорами, партнерами та громадськістю. Заборонено використовувати неофіційні канали для передачі службової інформації.

7.2 Соціальні мережі: Контент для соціальних мереж розміщується лише уповноваженими співробітниками. Заборонено використання особистих акаунтів для офіційних цілей. Публікація інформації про проекти фонду повинна супроводжуватися згодою всіх зацікавлених сторін (наприклад, бенефіціарів або партнерів). Заборонено публікувати неперевірену або конфіденційну інформацію.

7.3 Контроль контенту: Усі публікації повинні відповідати етичним стандартам фонду та не містити конфіденційної інформації.

7.4. Використання офіційних акаунтів:

- Лише уповноважені співробітники мають доступ до офіційних акаунтів фонду в соціальних мережах і на інших цифрових платформах.
- Доступ до акаунтів передається через безпечні способи і лише після затвердження керівництвом.

7.5. Архівування та збереження:

- Вся комунікація через офіційні канали має архівуватися для забезпечення прозорості та подальшого аналізу.
- Заборонено видаляти службову кореспонденцію без узгодження.

8. Відповідальність за порушення

8.1. Порушення цієї політики може призвести до:

- Усного чи письмового попередження.
- Обмеження доступу до ІКТ фонду.
- Розірвання співпраці у разі грубих порушень.
- Дисциплінарної відповідальності.
- Адміністративної відповідальності.

- Грошове стягнення (за розголошення конфіденційної інформації, комерційної таємниці).

9. Політика у разі надзвичайних ситуацій

- 9.1. У разі виявлення загроз для ІКТ (вірусів, хакерських атак) фонд негайно проводить заходи для нейтралізації загрози.
- 9.2. Розробляється план дій для відновлення інформаційних систем у разі їх пошкодження.
- 9.3. Усі співробітники проходять інструктаж щодо дій у разі надзвичайних ситуацій

10. Заключні положення

- 10.1. Політика є обов'язковою для виконання всіма працівниками, волонтерами та підрядниками фонду.
- 10.2. Зміни та доповнення до політики затверджуються керівництвом фонду.