ЗАТВЕРДЖЕНО:

Наказом виконавчого директора
БЛАГОДІЙНОЇ ОРГАНІЗАЦІЇ
«БЛАГОДІЙНИЙ ФОНД «КУЛЬТУРНІ
СИЛИ УКРАЇНИ» № 13 від 01.12.2025 року



_____ / Марія СКВОРЦОВА /

ПОЛІТИКА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

БЛАГОДІЙНА ОРГАНІЗАЦІЯ

«БЛАГОДІЙНИЙ ФОНД «КУЛЬТУРНІ СИЛИ УКРАЇНИ»

(код ЄДРПОУ: 45105021)

м. Київ – 2025 рік

ЗМІСТ

1. ЗАГАЛЬНІ ПОЛОЖЕННЯ 3
2. МЕТА ТА СФЕРА ЗАСТОСУВАННЯ 3
2.1. Мета 3
2.2. Сфера дії 3
3. ВИЗНАЧЕННЯ ТА АБРЕВІАТУРИ 3
4. СТАНДАРТИ ТА ПРАВИЛА КОРИСТУВАННЯ 4
4.1. Створення нового користувача 4
4.2. Видалення користувача 4
4.3. Використання обладнання 4
4.4. Доступ до ресурсів ІТ 5
4.5. Підключення зовнішніх пристроїв 5
4.6. Безпека комп'ютера, ПЗ і ЛКМ 5
4.7. Правила створення паролів 5
4.8. Підключення Wi-Fi 5
4.9. Доступ до інтернет-ресурсів організації 6
4.10. Резервне копіювання інформації 6
5. ВІДПОВІДАЛЬНІСТЬ ТА САНКЦІЇ 6

1. ЗАГАЛЬНІ ПОЛОЖЕННЯ

Комп'ютерна безпека є ключовою умовою ефективної роботи організації. Дотримання правил дозволяє захистити дані, попередити втрату інформації, уникнути неправомірного доступу та збоїв у роботі.

У Благодійній організації **«БФ «Культурні сили України»** використовується локальна комп'ютерна мережа (ЛКМ), яка забезпечує доступ до внутрішніх ресурсів: системи управління ресурсами, прикладних програм, електронної пошти, файлів, принтерів тощо. ЛКМ підключена до інтернету та використовується великою кількістю користувачів, тому її стабільність залежить від виконання встановлених правил.

Невиконання цих правил може спричинити порушення функціонування ЛКМ і, відповідно, роботи організації.

2. МЕТА ТА СФЕРА ЗАСТОСУВАННЯ

2.1. Мета

Правила визначають:

- безпечну та коректну роботу користувачів з комп'ютером, ЛКМ та інтернетом;
- забезпечення стабільної роботи ЛКМ та доступу до інтернету.

2.2. Сфера дії

Правила застосовуються до:

- усіх комп'ютерів та пристроїв організації;
- локальної комп'ютерної мережі;
- користувачів ПЗ та ІТ-інфраструктури.

3. ВИЗНАЧЕННЯ ТА АБРЕВІАТУРИ

Організація – Благодійна організація «БФ «Культурні сили України».

ЛКМ – Локальна комп'ютерна мережа.

ПЗ – Програмне забезпечення.

ІТ – Інформаційні технології.

Системне ПЗ – операційна система, BIOS, драйвери тощо.

Стандартне ПЗ – антивірус, архіватори, Word, Excel, PowerPoint, Outlook тощо.

Ресурси ІТ – обладнання, ЛКМ, системне, стандартне та прикладне ПЗ.

Користувач – особа, яка працює з комп'ютером, ЛКМ або інтернетом.

Робочі години – 10:00–19:00 (пн–пт).

4. СТАНДАРТИ ТА ПРАВИЛА КОРИСТУВАННЯ

4.1. Створення нового користувача

4.1.1. Отримати відділом кадрів дані нового співробітника:

- ПІБ;
- особиста електронна адреса;
- перелік груп доступу.

4.1.2. Створити обліковий запис і додати до відповідних груп.

4.1.3. Підготувати обладнання (комп'ютер, принтер тощо).

4.1.4. Ознайомити користувача з правилами, перевірити розуміння.

4.1.5. Видати обладнання.

4.1.6. Допомогти змінити пароль і налаштувати багаторівневу аутентифікацію.

4.1.7. Налаштувати підключення до ЛКМ або Wi-Fi.

4.2. Видалення користувача

4.2.1. Отримати лист щодо звільнення.

4.2.2. Заблокувати обліковий запис.

4.2.3. Прийняти все обладнання.

4.2.4. Перевірити комплектність та працездатність.

4.3. Використання обладнання

Кожен користувач несе особисту відповідальність за цілісність і працездатність виданого йому обладнання.

4.4. Доступ до ресурсів IT

- доступ регламентований і захищений паролями;
- час доступу необмежений, окрім періодів технічних робіт.

4.5. Підключення зовнішніх пристроїв

Дозволено підключати лише пристрої, перевірені антивірусом:

USB, SD-карти, зовнішні HDD тощо.

4.6. Безпека комп'ютера, ПЗ і ЛКМ

Забороняється:

- передавати паролі та ідентифікатори;
- лишати комп'ютер без нагляду більше ніж на 10 хвилин;
- працювати без антивірусу;
- вносити зміни у системні файли;
- встановлювати неавторизоване ПЗ;
- використовувати робочий інтернет у неметевих цілях;
- відвідувати небезпечні сайти;
- поширювати чутливу інформацію;
- користуватися незахищеними месенджерами;
- передавати доступ стороннім.

4.7. Правила створення паролів

- мінімум 8 символів;
- щонайменше 3 з 4 типів символів:
  - великі літери,
  - малі літери,
  - цифри,
  - спеціальні символи;
- пароль має бути закріплений за номером телефону.

4.8. Підключення Wi-Fi

Доступні мережі:

- **CF_WLAN** — для співробітників (доступ до ЛКМ);
- **CF_WLAN_Guest** — для гостей.

Забороняється передавати пароль від CF_WLAN стороннім.

4.9. Доступ до інтернет-ресурсів організації

Надається за погодженням керівництва через електронний лист до ІТ-спеціаліста.

4.10. Резервне копіювання інформації

Необхідно щотижня робити резервні копії на зовнішні носії та зберігати їх окремо.

5. ВІДПОВІДАЛЬНІСТЬ ТА САНКЦІЇ

У разі систематичного порушення правил ІТ-спеціалісти мають право обмежити або відключити користувача від ресурсів ІТ.