БЛАГОДІЙНА ОРГАНІЗАЦІЯ
«БЛАГОДІЙНИЙ ФОНД
«ДОБРОБУТ УКРАЇНИ»
ЄДРПОУ 40234987
61018, Україна, м. Харків,
вул. Отакара Яроша, 61-А, к. 10

CHARITABLE ORGANIZATION
«CHARITABLE FOUNDATION
«EUDEMONY OF UKRAINE»
№ 40234987
Otakara Yarosha street 61-A ap. 10 Kharkiv
Ukraine 61018

№27 від 30.09.2025

Н А К А З

Про затвердження Політики інформаційної та кібербезпеки

З метою забезпечення належного рівня кібербезпеки та інформаційної безпеки, захисту інформаційних активів, персональних даних, фінансової та іншої конфіденційної інформації, підвищення стійкості Організації до кіберзагроз, розвитку безпечних практик використання цифрових технологій та забезпечення безперервності діяльності Благодійної організації «Благодійний фонд «Добробут України», керуючись Статутом Організації,

НАКАЗУЮ:

1. Затвердити Політику інформаційної та кібербезпеки Благодійної організації «Благодійного фонду “Добробут України» (додається).
2. Контроль за виконанням даного наказу покласти на Офіцера з моніторингу та оцінки Організації

Голова Правління **Вікторія ПРЕОБРАЖЕНСЬКА**

З Наказом ознайомлені:

Офіцер з моніторингу та оцінки
Іоанн ПРЕОБРАЖЕНСЬКИЙ

Дата: «30» вересня 2025 р.

ЗАТВЕРДЖЕНО
Наказом Голови Правління

БО “БФ «ДОБРОБУТ УКРАЇНИ»
від 30.09.2025 №27

ПОЛІТИКА ІНФОРМАЦІЙНОЇ ТА КІБЕРБЕЗПЕКИ БЛАГОДІЙНОЇ ОРГАНІЗАЦІЇ «БЛАГОДІЙНИЙ ФОНД “ДОБРОБУТ УКРАЇНИ»

м. Київ – 2025 рік

tel. +380954152277 https://cfdobrobutua.weblium.site e-mail: info@dobrobutua.org
Р/р UA613515330000026007052221644 в ПАТ КБ «Приват Банк» у м. Київ МФО 351533

1. ЗАГАЛЬНІ ПОЛОЖЕННЯ
1.1. Ця Політика визначає підходи, принципи та зобов'язання Благодійної організації «Благодійний фонд «Добробут України» (далі – Організація) щодо забезпечення інформаційної та кібербезпеки у своїй діяльності.
1.2. Організація визнає, що інформація, цифрові ресурси, електронні системи, персональні дані, фінансова інформація та інші конфіденційні відомості є важливими активами Організації та потребують належного захисту від втрати, пошкодження, несанкціонованого доступу, розголошення або знищення.
1.3. Організація прагне впроваджувати розумні та пропорційні заходи захисту інформації та цифрових ресурсів відповідно до масштабу діяльності, наявних ресурсів, оцінених ризиків та вимог законодавства України і донорів.
1.4. Політика поширюється на працівників/ць, волонтерів/ок, консультантів/ок, членів Правління, підрядників, партнерів та інших осіб, які мають доступ до інформаційних ресурсів Організації.
1.5. Політика застосовується до всіх інформаційних систем, пристроїв, електронної пошти, хмарних сервісів, баз даних, цифрових платформ та інших інформаційних ресурсів, які використовуються Організацією.
1.6. Ця Політика застосовується у взаємозв'язку з Політикою захисту персональних даних, Політикою зберігання фінансових документів, Політикою управління ризиками, Політикою протидії фінансуванню тероризму та відмиванню коштів, Стандартом боротьби з неправомірними діями, Політикою safeguarding та іншими внутрішніми документами Організації.

2. ТЕРМІНИ ТА ВИЗНАЧЕННЯ
2.1. Інформаційна безпека - стан захищеності інформації від несанкціонованого доступу, зміни, знищення, втрати або розголошення.
2.2. Кібербезпека - сукупність організаційних, технічних та інших заходів, спрямованих на захист інформації, інформаційних систем та цифрових ресурсів від кіберзагроз.
2.3. Кіберінцидент - подія, яка може призвести або призвела до порушення безпеки інформаційних систем, даних або цифрових ресурсів.
2.4. Конфіденційна інформація — інформація, доступ до якої обмежено відповідно до законодавства України або внутрішніх документів Організації.

3. МЕТА ТА ЗАВДАННЯ ПОЛІТИКИ
3.1. Метою цієї Політики є забезпечення належного рівня захисту інформації, цифрових ресурсів та інформаційних систем Організації, а також підтримка безперервності діяльності Організації.
3.2. Організація прагне:
- запобігати несанкціонованому доступу до інформації;
- захищати персональні дані та конфіденційну інформацію;
- мінімізувати ризики втрати або пошкодження даних;
- підвищувати обізнаність працівників/ць щодо кіберзагроз;

- забезпечувати своєчасне реагування на кіберінциденти;
- підтримувати безпечне використання цифрових технологій.

4. ПРИНЦИПИ ОРГАНІЗАЦІЇ

4.1. Конфіденційність: Організація прагне забезпечувати доступ до інформації лише для осіб, які мають відповідні повноваження та службову необхідність.
4.2. Цілісність інформації: Організація прагне захищати інформацію від несанкціонованих змін, спотворення або знищення.
4.3. Доступність інформації: Організація прагне забезпечувати доступність інформації та систем для уповноважених осіб у межах виконання їхніх обов'язків.
4.4. Мінімально необхідний доступ: доступ до інформації та цифрових ресурсів надається лише в обсязі, необхідному для виконання робочих функцій.
4.5. Управління ризиками: Організація прагне враховувати ризики інформаційної безпеки та впроваджувати пропорційні заходи для їх запобігання та мінімізації.
4.6. Підзвітність та відповідальність: Кожна особа, яка має доступ до інформаційних ресурсів Організації, несе відповідальність за їх належне та безпечне використання.

5. БЕЗПЕЧНЕ ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ РЕСУРСІВ

5.1. Працівники/ці зобов'язані використовувати надійні паролі довжиною не менше 12 символів, що містять літери, цифри та спеціальні символи. Паролі мають бути унікальними для робочих облікових записів і не можуть передаватися третім особам. У разі підозри на компрометацію пароль негайно змінюється.
5.2. Двофакторна автентифікація (MFA) застосовується для доступу до електронної пошти, хмарних сервісів та інших систем, що містять конфіденційну інформацію.
5.3. Пристрої, що використовуються для роботи з інформацією Організації, повинні бути захищені паролем або іншим способом автентифікації.
5.4. Працівники/ці повинні вживати розумних заходів для захисту пристроїв від втрати, крадіжки або несанкціонованого доступу.
5.5. Організація використовує ліцензійне програмне забезпечення. На всіх пристроях увімкнено автоматичне встановлення оновлень безпеки операційних систем та програмного забезпечення.
5.6. Конфіденційні дані зберігаються у хмарних сервісах (Google Workspace, KoboToolbox), які забезпечують шифрування даних під час зберігання. Передача даних здійснюється виключно захищеними каналами (HTTPS/TLS).
5.7. Працівники/ці та інші уповноважені особи повинні проявляти обачність під час відкриття електронних листів, посилань, вкладень та файлів із невідомих або неперевірених джерел, а також негайно повідомляти про підозрілі повідомлення чи спроби отримання конфіденційної інформації (фішинг).

5.8. На всіх робочих пристроях використовуються засоби антивірусного захисту та мережевий екран (зокрема вбудовані Microsoft Defender і брандмауер Windows) з увімкненим автоматичним оновленням.
5.9. Організація веде реєстр доступів до інформаційних систем із зазначенням осіб, систем та обсягу прав. Реєстр оновлюється при кадрових змінах; у разі припинення співпраці облікові записи деактивуються невідкладно. Права доступу періодично переглядаються.
5.10. Перед початком використання нового цифрового сервісу або залученням зовнішнього постачальника Організація перевіряє його політику конфіденційності та відповідність вимогам захисту даних (зокрема GDPR). Доступ зовнішніх осіб до інформаційних ресурсів надається за принципом мінімально необхідного.

6. ФІЗИЧНА БЕЗПЕКА
6.1. Офіси Організації зачиняються;
6.2. Доступ до офісів та ключі має обмежене коло працівників/ць
6.3. Відвідувачі перебувають у приміщеннях лише у супроводі працівників/ць;
6.4. Серверне та мережеве обладнання розміщується в окремому зачиненому приміщенні;
6.5. Паперові документи з конфіденційною інформацією зберігаються у сейфі.

7. РЕЗЕРВНЕ КОПІЮВАННЯ ТА ЗБЕРЕЖЕННЯ ІНФОРМАЦІЇ
7.1. Організація прагне забезпечувати резервне копіювання важливої інформації та документів у спосіб, що відповідає її ресурсам та технічним можливостям.
7.2. Резервне копіювання критично важливих даних здійснюється регулярно.
7.3. Важливі документи та дані зберігаються у визначених Організацією місцях або системах зберігання.
7.4. Зберігання фінансових документів здійснюється відповідно до Політики зберігання фінансових документів та інших внутрішніх процедур Організації.

7. РЕАГУВАННЯ НА КІБЕРІНЦИДЕНТИ
7.1. Працівники/ці та інші залучені особи повинні негайно повідомляють відповідальну особу з питань інформаційної безпеки - Офіцера з моніторингу та оцінки про підозрілі електронні листи, втрату пристроїв, підозру на несанкціонований доступ, витік інформації або інші події, які можуть свідчити про кіберінцидент.
7.2. Після повідомлення відповідальна особа проводить оцінку масштабу інциденту, вживає заходів стримування (зміна паролів, блокування доступів), проводить розслідування та документування. Керівництво інформується невідкладно; донори — за потреби. За результатами розслідування складається звіт для керівництва та, за потреби, донора.

7.3. У разі необхідності Організація може залучати зовнішніх фахівців або компетентні органи для розслідування кіберінцидентів.

8. НАВЧАННЯ ТА ПІДВИЩЕННЯ ОБІЗНАНОСТІ
8.1. Організація проводить інструктаж з кібербезпеки для нових працівників/ць перед початком роботи та щорічне навчання для всіх працівників/ць.
8.2. Періодично надсилаються інформаційні повідомлення щодо актуальних кіберзагроз та заходів їх запобігання.
8.3. Працівники/ці та інші залучені особи заохочуються до дотримання належних практик цифрової безпеки та відповідального використання інформаційних ресурсів.

9. МОНІТОРИНГ ТА ПЕРЕГЛЯД ПОЛІТИКИ
9.1. Контроль за виконанням цієї Політики здійснює відповідальна особа з питань інформаційної безпеки.
9.2. Відповідальна особа щонайменше раз на рік проводить огляд основних ризиків кібербезпеки (управління доступами, резервне копіювання, фішинг та інші актуальні загрози) і подає висновки керівництву.
9.3. Політика переглядається та оновлюється щонайменше раз на рік та позачергово за потреби, зокрема у разі зміни вимог законодавства чи донорів, суттєвих змін у діяльності Організації або після кіберінцидентів.

10. ПРИКІНЦЕВІ ПОЛОЖЕННЯ
10.1. Політика набуває чинності з дня її затвердження наказом Голови Правління.
10.2. Усі працівники/ці та інші залучені особи ознайомлюються з Політикою під підпис.

Голова Правління **Вікторія ПРЕОБРАЖЕНСЬКА**

З Політикою ознайомлені:

Офіцер з моніторингу та оцінки
Іоанн ПРЕОБРАЖЕНСЬКИЙ Дата: «30» вересня 2025р.

tel. +380954152277 https://cfdobrobutua.weblium.site e-mail: info@dobrobutua.org
Р/р UA613515330000026007052221644 в ПАТ КБ «Приват Банк» у м. Київ МФО 351533