ЗАТВЕРДЖЕНО
від 29 березня 2024 року
Голови Фонду
БЛАГОДІЙНОЇ ОРГАНІЗАЦІЇ
“БЛАГОДІЙНИЙ ФОНД “ВІТРИ ЗМІН”

_____
Наталія ВЕГРИЯН

ПОЛІТИКА ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ БЛАГОДІЙНОЇ ОРГАНІЗАЦІЇ “БЛАГОДІЙНИЙ ФОНД “ВІТРИ ЗМІН” (Код ЄДРПОУ 42146311)

1. ЗАГАЛЬНІ ПОЛОЖЕННЯ

1.1. Ця **Політика технічного захисту інформації БЛАГОДІЙНОЇ ОРГАНІЗАЦІЇ “БЛАГОДІЙНИЙ ФОНД “ВІТРИ ЗМІН” (далі - Політика, Фонд)** містить положення, які визначають загальний порядок, процедури та особливості запровадження і підтримки інформаційної безпеки Фонду, виявлення та керування ризиками в інформаційній системі Фонду, упорядкування обсягів та рівнів доступу до здійснення окремих операцій, пов'язаних зі збиранням, обробкою, зберіганням, передачею та/або захистом інформації, а також вирішення інших технічних питань у площині гарантування цілісності та недоторканності внутрішнього інформаційного простору Фонду.

Метою затвердження цієї Політики є закріплення принципів та підходів до створення безпечних технічних та технологічних умов експлуатації інформаційної системи Фонду у межах виконання завдань статутної (благодійної) діяльності останнього з неухильним дотриманням прав та законних інтересів бенефіціарів, учасників, працівників, волонтерів, контрагентів, партнерів Фонду у сфері інформаційних правовідносин, а також запобігання несанкціонованому доступу до інформації з боку третіх осіб, неконтрольованому поширенню, викраденню, викривленню, втраті інформації та/або вчиненню інших протиправних дій/бездіяльності, спрямованих на порушення чинного законодавства України та/або міжнародних актів з питань захисту інформації.

1.1.2. **Предметом захисту цієї Політики** з урахуванням ч. 1 ст. 1 **Закону України “Про інформацію” від 02.10.1992 року № 2657-XII (далі - ЗУ № 2657)** виступає **інформація**, а саме будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді, знаходяться у володінні Фонду з метою належного провадження ним своєї статутної (благодійної) діяльності, і підлягають захисту шляхом, зокрема застосування тих чи інших організаційних та/або інженерно-технічних засобів у порядку та на умовах, визначених Політикою.

До предмету захисту цієї Політики включаються наступні види інформації:
- конфіденційна інформація, обсяг якої визначається Фондом відповідно до ч. 2 ст. 21 **ЗУ № 2657;**
- комерційна таємниця, обсяг якої визначається Фондом відповідно до ч. 2 ст. 505 **Цивільного кодексу України (далі - ЦКУ);**
- персональні дані, обсяг яких визначається Фондом відповідно до ст. 2 **Закону України “Про захист персональних даних” від 01.06.2010 року № 2297-VI (далі - ЗУ № 2297).**

Інформація, яка є предметом захисту цієї Політики та знаходиться у володінні Фонду, збирається, зберігається, обробляється ним **у паперовій та/або електронній формі**, якщо інше не визначено чинним законодавством України, рішенням Голови Фонду та/або вимогами грантодавців (донорів).

1.1.3. Положення цієї Політики одночасно застосовуються на двох взаємопов'язаних рівнях, а саме:
- **внутрішній рівень** - дотримання Політики є обов’язковим для всіх учасників, у тому числі членів органів управління, та працівників Фонду, до кола статутних/трудових обов’язків яких віднесено питання, пов’язані з використанням та/або захистом інформації, володільцем якої виступає Фонд.
- **зовнішній рівень** - дотримання Політики є обов’язковим для всіх волонтерів, контрагентів, партнерів Фонду, до кола цивільно-правових/господарсько-правових обов’язків яких віднесено питання, пов’язані з використанням та/або захистом інформації, володільцем якої виступає Фонд.

Бенефіціари, а також контрагенти/партнери Фонду, які безпосередньо не беруть участь у виконанні завдань статутної (благодійної) діяльності Фонду, зобов’язані дотримуватись вимог цієї Політики у випадках, коли у процесі реалізації Фондом завдань вказаної діяльності вони передають Фонду будь-яку інформацію, яка входить до предмету захисту цієї Політики, в електронній формі з використанням спеціальних технічних засобів та/або програмного забезпечення.

1.2. Положення цієї Політики розроблені на підставі актів системи чинного законодавства України, зокрема:

- ЦКУ;
- ЗУ № 2657;
- ЗУ № 2297;
- Закону України "Про захист інформації в інформаційно-комунікаційних системах" від 05.07.1994 року № 80/94-ВР (далі - ЗУ № 80/94);
- інших актів чинного законодавства України, предметом регулювання яких виступають питання інформаційної безпеки.

Політика орієнтована на запровадження та практичне застосування у межах Фонду положень міжнародних актів у сфері інформаційної безпеки, зокрема, але не виключно **Регламенту Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року** про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування директиви 95/46/ЄС, **Директиви Європейського Парламенту і Ради (ЄС) 2016/1148 від 6 липня 2016 року** про заходи для високого спільного рівня безпеки мережевих та інформаційних систем на території Союзу тощо у частині, яка є/може бути застосовною до побудови процесів підтримки інформаційної безпеки у межах Фонду.

Положення Політики ґрунтуються на Статуті Фонду, а також враховують зміст положень його інших внутрішніх (локальних) актів, зокрема:

- Політики захисту персональних даних Фонду;
- Політики закупівель Фонду;
- Політики отримання та використання благодійної/гуманітарної допомоги Фонду;
- інших внутрішніх (локальних) актів Фонду, які регулюють порядок провадження статутної (благодійної) діяльності Фонду з метою врахування особливостей провадження вказаної діяльності, які впливають на обрання і подальше застосування технічних способів, засобів, методів, інструментів використання і захисту інформації, яка знаходиться у володінні Фонду.

1.3. Положення цієї Політики розроблені з урахуванням технічних рекомендацій, висвітлених у Державних стандартах України (далі - ДСТУ), гармонізованих з європейськими та міжнародними стандартами у сфері інформаційної безпеки, та нормативних документах технічного захисту інформації (далі - НД ТЗІ), затверджених Адміністрацією Державної служби спеціального зв'язку та захисту інформації України, а саме:

- ДСТУ ISO/IEC 27000:2019 "Інформаційні технології. Методи захисту. Системи керування інформаційною безпекою. Огляд і словник термінів";
- ДСТУ ISO/IEC 27005:2019 "Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки";
- ДСТУ ISO/IEC TS 27008:2019 "Інформаційні технології. Методи захисту. Настанова щодо оцінювання захисту інформаційної безпеки";
- ДСТУ ISO/IEC 27018:2019 "Інформаційні технології. Методи захисту. Кодекс усталеної практики для захисту персональної ідентифікаційної інформації (PII) у загальнодоступних хмарах, що діють як процесори PII";
- НД ТЗІ 3.6-004-21 "Порядок впровадження системи безпеки інформації в державних органах, на підприємствах, організаціях, в інформаційно-комунікаційних системах яких обробляється інформація, вимога щодо захисту якої встановлена законом та не становить державної таємниці";
- НД ТЗІ 3.6-006-21 "Порядок вибору заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем";
- інші ДСТУ у сфері захисту інформації та інформаційної безпеки та НД ТЗІ.

1.4. Практичне застосування положень Політики має здійснюватись з неухильним дотриманням наступних принципів:

- **Доступність інформації** - весь процес використання та захисту інформації, яка знаходиться у володінні Фонду, має виключати будь-яку можливість, зокрема, але не виключно, неавторизованого блокування інформації та/або інформаційної системи Фонду, та/або окремих складових зазначеної системи без наявності підстав, визначених чинним законодавством України та/або Політикою.

- **Цілісність інформації** - весь процес використання та захисту інформації, яка знаходиться у володінні Фонду, має виключати будь-яку можливість, зокрема, але не виключно, неавторизованого знищення, модифікації, переміщення, та/або будь-якого іншого втручання у зміст, форму, спосіб викладення, систематизації та/або будь-які інші формально-змістовні складові вказаної інформації з боку та/або на користь третіх осіб без наявності підстав, визначених чинним законодавством України та/або Політикою.

- **Конфіденційність** - весь процес використання та захисту інформації, яка знаходиться у володінні Фонду, має виключати будь-яку можливість, зокрема, але не виключно, неавторизованого доступу, копіювання, надання та/або розповсюдження зазначеної інформації з боку та/або на користь третіх осіб без наявності підстав, визначених чинним законодавством України та/або Політикою.

1.5. Терміни вживаються у цій Політиці у наступному значенні:

- **"Власник інформаційної системи"** - з урахуванням ст. 1 **ЗУ № 80/94** фізична або юридична особа, якій належить право власності на інформаційну систему.

Для цілей цієї Політики власником інформаційної системи визнається Фонд, якщо інше прямо не зазначено та/або не випливає із положень Політики.

- **"Володілець інформації"** - з урахуванням ст. 1 **ЗУ № 80/94** фізична або юридична особа, якій належать права на інформацію.

Для цілей цієї Політики володільцем інформації визнається Фонд, якщо інше прямо не зазначено та/або не випливає із положення/положень Політики.

- **"Доступ до інформації в системі"** - з урахуванням ст. 1 **ЗУ № 80/94** отримання користувачем можливості обробляти інформацію в системі.

- **"Захист інформації в системі"** - з урахуванням ст. 1 **ЗУ № 80/94** діяльність, спрямована на запобігання несанкціонованим діям щодо інформації в системі.

- **"Знищення інформації в системі"** - з урахуванням ст. 1 **ЗУ № 80/94** дії, внаслідок яких інформація в системі зникає.

- **"Інформаційна (автоматизована) система" (далі - система)** - з урахуванням ст. 1 ЗУ № 80/94 організаційно-технічна система, в якій реалізується технологія обробки інформації з використанням технічних і програмних засобів Фонду.

- **"Інформаційні ресурси Фонду"** - засоби та інструменти, за допомогою яких Фонд здійснює збирання інформації та/або поширення інформації, володільцем якої він є, у тому числі у процесі комунікації з бенефіціарами Фонду, з метою виконання завдань власної статутної (благодійної) діяльності та/або реалізації окремих благодійних проєктів/програм Фонду (зокрема, офіційний веб-сайт Фонду, Instagram, Telegram, WhatsApp, Facebook тощо).

- **"Комплексна система захисту інформації"** - з урахуванням ст. 1 **ЗУ № 80/94** взаємопов'язана сукупність організаційних та інженерно-технічних заходів, засобів і методів захисту інформації, володільцем якої виступає Фонд.

- **"Конфіденційною інформація"** - з урахуванням ч. 2 ст. 21 **ЗУ № 2657** інформація про фізичну особу, інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень, а також інформація, визнана такою на підставі закону.

- **"Користувач інформації в системі"** - з урахуванням ст. 1 **ЗУ № 80/94** фізична або юридична особа, яка в установленому законодавством порядку отримала право доступу до інформації в системі.

У розумінні цієї Політики користувачами інформації в системі виступають учасники, працівники, волонтери та/або контрагенти Фонду, які безпосередньо беруть участь у виконанні завдань статутної (благодійної) діяльності Фонду.

- **"Несанкціоновані дії щодо інформації в системі"** - з урахуванням ст. 1 **ЗУ № 80/94** дії, що провадяться з порушенням порядку доступу до цієї інформації, установленого відповідно до законодавства та цієї Політики.

- **"Обробка інформації в системі"** - з урахуванням ст. 1 **ЗУ № 80/94** виконання однієї або кількох операцій, зокрема: збирання, введення, записування, перетворення, зчитування, зберігання, знищення, реєстрації, приймання, отримання, передавання, які здійснюються в системі за допомогою технічних і програмних засобів Фонду.

- **"Персональні дані"** - з урахуванням ст. 2 **ЗУ № 2297** відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована.

- **“Порушення цілісності інформації в системі”** - з урахуванням ст. 1 **ЗУ № 80/94** несанкціоновані дії щодо інформації в системі, внаслідок яких змінюється її вміст.

- **“Порядок доступу до інформації в системі”** - з урахуванням ст. 1 **ЗУ № 80/94** умови отримання користувачем можливості обробляти інформацію в системі та правила обробки цієї інформації, визначені відповідно до цієї Політики.

- **“Програмне забезпечення”** - сукупність програм системи оброблення інформації та програмних документів, необхідних для експлуатації цих програм, які використовуються Фондом під час використання інформації, яка знаходиться у володінні останнього.

- **“Технічні засоби”** - обладнання, апаратура та/або пристрої (зокрема, ноутбуки, персональні комп’ютери, планшети, смартфони тощо), які застосовуються Фондом у межах системи з метою належного виконання операцій з інформацією, яка знаходиться у володінні Фонду.

Інші терміни вживаються у Політиці у значенні, встановленому нормами актів чинного законодавства України, предметом регулювання яких є інформаційні правовідносини, а також у ДСТУ, НД ТЗІ.

1.6. У разі, якщо вимоги грантодавця (донора) Фонду містять більш суворі вимоги до організації порядку захисту інформації, яка знаходиться у володінні Фонду, ніж ті, які містяться у цій Політиці, застосуванню підлягають відповідні вимоги грантодавця (донора).

Враховуючи технічні та технологічні особливості процесів, пов’язаних з використанням та захистом інформації, яка знаходиться у володінні Фонду, порядок, способи та строки реалізації вимог грантодавця (донора), які вказані у цьому пункті, визначаються з урахуванням положень грантового договору (контракту) та не повинні призвести до порушення принципів, викладених у п. 1.6. Політики.

1.7. Предметом регулювання цієї Політики не є <u>юридичні аспекти та особливості</u>:
- збору, обробки, зберігання, видалення та захисту персональних даних у контексті положень ЗУ № 2297;
- використання і захисту конфіденційної інформації та комерційної таємниці Фонду у контексті положень ЦКУ, Господарського кодексу України та ЗУ № 2657.

1.8. Ця Політика діє безстроково з моменту її затвердження у порядку, передбаченому Статутом Фонду, якщо інше не визначено наказом Голови Фонду.

Перегляд положень Політики може бути проведено у будь-який час у залежності від поточних потреб та інтересів Фонду, вимог грантодавців (донорів), інших умов, що впливають на досягнення мети статутної (благодійної) діяльності Фонду, якщо інше не визначено наказом Голови Фонду.

Голова Фонду за власною ініціативою та/або за ініціативою грантодавців (донорів) Фонду уповноважений вносити зміни до положень Політики.

Внесення змін до положень Політики здійснюється на підставі видання відповідного наказу Голови Фонду.

Інформація про внесення змін до положень Політики може доводитись до відома зацікавлених осіб, зокрема, у спосіб, який використовувався під час публікації її первинної редакції, якщо інше не визначено Головою Фонду.

Строк опублікування зазначеної інформації визначається Головою Фонду.

2. ПРАВОВИЙ СТАТУС СУБ’ЄКТІВ ЗАСТОСУВАННЯ ПОЛІТИКИ

2.1. До органів/посадових осіб Фонду, яких наділено повноваженнями щодо вирішення питань, пов’язаних з практичним застосуванням положень цієї Політики, відносяться:
- Голова Фонду;
- Загальні збори Фонду.

2.1.1. За рішенням Загальних зборів Фонду може бути створено допоміжні органи, основним завданням яких є вирішення питань, пов’язаних з організацією інформаційної безпеки Фонду (Комісія, Комітет, Колегія тощо) (далі - Допоміжний орган).

Порядок та форми роботи, кількісний та особовий склад, особливості прийняття і оформлення рішень, інші особливості діяльності Допоміжного органу визначаються за рішенням Загальних зборів Фонду.

2.1.2. Фонд може залучити фізичну особу (осіб), до компетенції яких входить вирішення питань, пов'язаних з організацією інформаційної безпеки Фонду, у межах трудових правовідносин, на посади, які відповідають чинному Класифікатору професій та визначені у штатному розписі, затвердженому Головою Фонду у порядку, визначеному трудовим законодавством України та Статутом Фонду.

Повноваження осіб, вказаних у цьому пункті, визначаються відповідно до Довідника кваліфікаційних характеристик професій працівників та закріплюються у посадових інструкціях, затверджених Головою Фонду у порядку, визначеному трудовим законодавством України та Статутом Фонду.

2.1.3. Фонд може залучити особу (осіб), до компетенції яких входить вирішення питань, пов'язаних з організацією інформаційної безпеки Фонду, у межах:
- цивільно-правових відносин на підставі договору про надання послуг;
- господарсько-правових відносин на підставі договору про надання послуг, у тому числі договору з ФОП.

Права та обов'язки осіб, вказаних у цьому пункті, а також умови та вимоги Фонду до їх виконання визначаються у відповідних договорах та/або додатках до них з урахуванням положень цієї Політики та/або інших внутрішніх (локальних) актів Фонду, предмет регулювання яких дотичний до організації інформаційної безпеки Фонду.

2.1.4. Фонд може визначати вимоги до осіб, вказаних у пп. 2.2.2., 2.2.3. Політики (далі - Відповідальна особа), спрямовані на залучення до співпраці високопрофесійних фахівців у сфері інформаційної безпеки та захисту, інформаційних технологій (IT), кібербезпеки тощо.

До таких вимог, зокрема, можуть відноситись:
- наявність профільної вищої освіти;
- досвід професійної/трудової діяльності у відповідній сфері;
- володіння програмним забезпеченням, призначеним для організації, підтримки та/або моніторингу стану інформаційної безпеки та/або розробка зазначеного програмного забезпечення;
- наявність рекомендацій від третіх осіб, які мають попередній успішний досвід співпраці з відповідною особою-кандидатом;
- інші вимоги, визначені Фондом з метою відбору та залучення профільних фахівців, які відповідають актуальним потребам провадження статутної (благодійної) діяльності.

Вимоги, зазначені у цьому пункті, визначаються за рішенням Голови Фонду, а перевірка рівня відповідності їм кандидатів проводиться у порядку та на умовах, визначених внутрішніми (локальними) актами Фонду у сфері працевлаштування або проведення закупівель, та чинним законодавством України.

2.2. До повноважень Голови Фонду у сфері організації інформаційної безпеки відносяться:
- укладення трудових договорів з працівниками, які працевлаштовуються на посади у сфері забезпечення інформаційної безпеки Фонду;
- укладення цивільно-правових та/або господарських договорів, у тому числі договорів з ФОП, предметом яких виступає надання послуг у сфері забезпечення інформаційної безпеки Фонду;
- здійснення загального контролю за дотриманням та практичною реалізацією дотримання положень цієї Політики;
- визначення порядку генерування, обліку та зміни паролів доступу до технічних засобів та/або програмного забезпечення у межах інформаційної системи Фонду у межах та порядку, визначеному Політикою;
- визначення порядку здійснення резервного копіювання та відновлення інформації, володільцем якої виступає Фонд, у межах та порядку, визначеному Політикою;
- вирішення інших питань, пов'язаних з організацією інформаційної безпеки Фонду, які прямо передбачені Політикою та/або які не відносяться до компетенції інших органів/посадових осіб Фонду.

За рішенням Голови Фонду частина його повноважень, пов'язана з практичним застосуванням положень Політики, може бути делегована уповноваженій особі у порядку, визначеному чинним законодавством України.

2.3. Загальні збори Фонду можуть приймати рішення з будь-яких питань, пов'язаних з практичною реалізацією цієї Політики, у порядку, визначеному Статутом Фонду.

2.4. Зміна повноважень органів/посадових осіб Фонду у сфері організації інформаційної безпеки Фонду та/або порядку залучення осіб для виконання завдань цієї Політики на підставі трудових, цивільно-правових та/або господарських договорів, у тому числі договорів з ФОП, здійснюється шляхом внесення відповідних змін до Політики за рішенням Голови Фонду.

2.5. Учасники, працівники, волонтери, контрагенти Фонду, які беруть участь у виконанні завдань його статутної (благодійної) діяльності, зобов'язані:

- неухильно дотримуватись цієї Політики під час виконання професійних, службових або трудових обов'язків у межах використання інформації, володільцем якої виступає Фонд, під час та/або за результатами участі у виконанні завдань статутної (благодійної) діяльності Фонду;
- запобігати втраті інформації, володільцем якої виступає Фонд, її неправомірному використанню, вилученню, викривленню, несанкціонованому поширенню тощо;
- не розголошувати інформацію, володільцем якої виступає Фонд, яка була довірена їм або яка стала відома у зв'язку з виконанням професійних, службових або трудових обов'язків (таке зобов'язання залишається чинним після припинення ними співпраці з Фондом, крім випадків, встановлених чинним законодавством України);
- повідомляти Голову Фонду та/або уповноважену ним особу, та/або Допоміжний орган, та/або Відповідальну особу про всі факти порушення та/або реальної загрози порушення цієї Політики, сприяти встановленню обставин зазначеного порушення шляхом надання інформації, яка була зафіксована у будь-якій формі, про обставини допущення порушення та/або джерела отримання зазначеної інформації тощо;
- брати участь у проведенні періодичних заходів, присвячених підвищенню обізнаності та/або професійних навичок роботи з інформацією, володільцем якої виступає Фонд, серед учасників, працівників, волонтерів, контрагентів Фонду;
- виконувати інші обов'язки, визначені положеннями чинного законодавства України та/або міжнародних актів у сфері інформаційної безпеки, та/або які випливають з цієї Політики.

2.6. Учасникам, працівникам, волонтерам, контрагентам Фонду, які беруть участь у виконанні завдань його статутної (благодійної) діяльності, забороняється:
- надавати паролі, які використовуються у межах отримання доступу до інформації, володільцем якої є Фонд, третім особам, крім випадків, коли відповідне рішення прийнято Головою Фонду;
- самостійно здійснювати видалення, редагування, копіювання та/або будь-які інші операції з інформацією, володільцем якої є Фонд, без попереднього письмового повідомлення про це Голови Фонду та/або уповноваженої ним особи, та/або Допоміжного органу, та/або Відповідальної особи;
- надавати спільний доступ до технічних засобів, які знаходяться у їх власності і використовуються для обробки інформації, володільцем якої є Фонд, третім особам, крім випадків, коли відповідне рішення прийнято Головою Фонду;
- використовувати технічні засоби Фонду з будь-якою особистою метою, зокрема, але не виключно для спілкування з третіми особами поза межами виконання професійних, службових або трудових обов'язків, збору, обробки, зберігання та/або інших операцій з використання інформації, яка не має відношення до провадження статутної (благодійної) діяльності Фонду, вчинення електронних правочинів у сфері електронної комерції, не пов'язаних з виконанням завдань статутної (благодійної) діяльності Фонду, тощо;
- у процесі виконання своїх професійних, службових або трудових обов'язків користуватись особистими акаунтами у соціальних мережах, електронних поштах, "хмарних" сховищах та/або інших віртуальних засобах зберігання інформації тощо;
- користуватись відкритими мережами Wi-Fi поза межами Фонду, крім випадків, коли операції з використання інформації, володільцем якої є Фонд, мають бути здійснені невідкладно, а захищений доступ до мережі Інтернет є об'єктивно недоступним;
- користуватись під час обробки інформації, володільцем якої є Фонд, технічними засобами, програмне забезпечення яких є застарілим та не відповідає сучасним стандартам інформаційної та кібернетичної безпеки;
- вчиняти інші дії, які підвищують ризик та/або потенційно можуть призвести до допущення порушень цієї Політики.

3. КОМПЛЕКСНА СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ ФОНДУ: ЗАГАЛЬНІ ПОЛОЖЕННЯ

3.1. Засоби захисту інформації, володільцем якої є Фонд, які запроваджені та використовуються ним на практиці у межах певного проміжку часу, виступають складовими частинами **комплексної системи захисту інформації Фонду.**

З метою забезпечення високого рівня інформаційної безпеки Фонду останнім можуть застосовуватись будь-які засоби організаційного та інженерно-технічного захисту інформації, яка знаходиться у володінні Фонду, з урахуванням:
- поточних потреб статутної (благодійної) діяльності Фонду;
- форм, способів та/або засобів збирання, обробки та/або зберігання інформації, володільцем якої є Фонд;
- наявності та/або рівня ризиків втрати, викривлення, викрадення та/або несанкціонованого розповсюдження інформації, володільцем якої є Фонд;
- вимог та/або умов грантодавців (донорів) Фонду у рамках виконання окремих грантових договорів (контрактів);
- інших обставин, які впливають на ступінь забезпечення захисту інформації, володільцем якої є Фонд, відповідно до цієї Політики.

3.1.1. До організаційних засобів захисту інформації, яка знаходиться у володінні Фонду, відносяться, зокрема:

- процедури призначення та/або залучення фахівців у сфері технологій захисту інформації, кібербезпеки;
- процедури підвищення обізнаності учасників, працівників, волонтерів та контрагентів Фонду у сфері технологій захисту інформації, кібербезпеки;
- процедури виявлення та реагування на факти несанкціонованих операцій з інформацією, володільцем якої виступає Фонд, та/або інших порушень цієї Політики;
- інші процедури, спрямовані на практичну реалізацію положень Політики та досягнення мети її запровадження.

Організаційні засоби захисту інформації, володільцем якої виступає Фонд, визначаються положеннями цієї Політики та/або рішеннями Голови Фонду, та/або вимогами грантодавців (донорів) Фонду.

3.1.2. До інженерно-технічних засобів захисту інформації, яка знаходиться у володінні Фонду відносяться, зокрема:

- керування доступом, що дає змогу контролювати доступ до інформації, яка знаходиться у володінні Фонду, як на матеріальних носіях, так і у "хмарних" сховищах;
- автентифікація, у тому числі двофакторна, користувачів інформаційної системи Фонду;
- резервне копіювання й відновлення інформації, яка знаходиться у володінні Фонду, для забезпечення до них доступу після збою у системі, їх пошкодження або аварії;
- видалення інформації, яка знаходиться у володінні Фонду, що дає змогу зробити її невідновною;
- програмне забезпечення для маскування даних, що приховує зміст інформації, яка знаходиться у володінні Фонду, від незареєстрованих/неавтентифікованих користувачів за допомогою проксі-символів;
- рішення для захисту від втрати даних, які запобігають несанкціонованому використанню інформації, яка знаходиться у володінні Фонду;
- шифрування, яке перетворює зміст інформації, яка знаходиться у володінні Фонду, на непридатний для читання незареєстрованими користувачами;
- керування внутрішніми ризиками у межах Фонду для зменшення небезпечних дій користувачів;
- інші засоби захисту, використання яких є необхідним у межах статутної (благодійної) діяльності Фонду.

Голова Фонду та/або уповноважена ним особа, та/або Допоміжний орган, та/або Відповідальна особа самостійно приймає рішення про використання та/або запровадження, та/або зміну тих чи інших інженерно-технічних засобів захисту у межах Фонду, у тому числі на виконання вимог грантодавців (донорів) Фонду.

3.2. Порядок та умови застосування засобів захисту інформації, володільцем якої є Фонд, запроваджених відповідно до п. 3.1. Політики, доводиться до відома всіх учасників, працівників, волонтерів та контрагентів Фонду, які безпосередньо беруть участь у виконанні завдань його статутної (благодійної) діяльності у порядку, визначеному Головою Фонду та/або уповноваженою ним особою.

Підтвердження обізнаності осіб, вказаних у цьому пункті, з положеннями Політики та/або особливості застосування вказаних положень у межах взаємовідносин між Фондом та окремо взятими особами може бути зафіксовано у письмовій/електронній формі шляхом:

а) Надання вказаними особами відповідної згоди-повідомлення **(далі - Згода-повідомлення)**;

б) Укладення між Фондом та вказаними особами **договорів про конфіденційність (далі - Договір)**, які визначають, зокрема:

- зміст та обсяг інформації, яка не підлягає розголошенню/несанкціонованому використанню;
- права, обов'язки та відповідальність сторін у контексті дотримання режиму захисту інформації, володільцем якої є Фонд;
- строк дійсності обов'язку дотримання цієї Політики вказаними особами після завершення строку дії Договору; інші особливості взаємовідносин сторін, які стосуються дотримання положень цієї Політики.

в) Включення положень, які стосуються обов'язку неухильного дотримання вказаними особами положень цієї Політики, до тексту трудових, цивільно-правових, господарських договорів, у тому числі договорів з ФОП/самозайнятими особами, договорів про провадження волонтерської діяльності, укладеними з Фондом.

Випадки та/або сфери, форма, строки та порядок застосування засобів підтвердження обізнаності осіб, вказаних у цьому пункті, з положеннями Політики та/або особливості застосування вказаних положень у межах взаємовідносин між Фондом та окремо взятими особами визначається Головою Фонду та/або уповноваженою ним особою.

4. ОРГАНІЗАЦІЙНІ ТА ІНЖЕНЕРНО-ТЕХНІЧНІ ЗАХОДИ ЗАХИСТУ ІНФОРМАЦІЇ

4.1. Для виконання операцій, пов'язаних з використанням інформації, володільцем якої є Фонд, учасники, працівники, волонтери та/або контрагенти Фонду **попередньо отримують доступ** до відповідної інформації у

порядку, визначеному цією Політикою та/або положеннями внутрішніх (локальних) актів Фонду, предметом регулювання яких виступають відповідні питання.

Доступ до інформації у паперовій та/або електронній формі для учасників, працівників, волонтерів та/або контрагентів Фонду, до повноважень/обов'язків яких входить обробка та/або зберігання такої інформації, надається їм на підставі:

- посадової інструкції та за наявності письмового трудового договору та/або договору про конфіденційність, що включають Згоду повідомлення - **для працівників Фонду**;
- цивільно-правового та/або господарського договору, у тому числі договору з ФОП, та/або Згоди-повідомлення, та/або договору про конфіденційність - **для контрагентів Фонду**;
- договору про провадження волонтерської діяльності, та/або Згоди-повідомлення, та/або договору про конфіденційність - **для волонтерів Фонду**;
- Згоди-повідомлення та/або договору про конфіденційність - **для учасників Фонду.**

4.1.1. Інформація, закріплена **у паперовій формі,** зберігається Фондом у спеціально відведеному приміщенні (сховищі), входи та/або виходи з/до якого містять магнітні замки та/або інші засоби контрольованого доступу.

Інформація, закріплена **у паперовій формі,** надається за запитом учасника, працівника, волонтера та/або контрагента Фонду, крім тих, які зазначені у п. 3.6. Політики, в обсязі, необхідному для належного виконання ним своїх професійних, службових, трудових та/або інших обов'язків.

Порядок та особливості доступу до інформації, закріпленої **у паперовій формі,** оформлення та подання відповідного запиту, фіксування фактів отримання доступу до інформації (дата, час надання доступу, обсяг, зміст отриманої інформації тощо), підстави для відмови у наданні доступу до інформації тощо визначаються за рішенням Голови Фонду.

Порядок надання, обліку, виготовлення, передачі та/або відновлення втрачених магнітних карток, ключів та/або інших засобів доступу до приміщення (сховища), вказаного у цьому пункті, учасників Фонду, працівників, волонтерів та/або контрагентів Фонду здійснюється у порядку, визначеному Головою Фонду та/або уповноваженою ним особою, та/або Допоміжним органом, та/або Відповідальною особою.

Доступ до приміщення (сховища), вказаного у цьому пункті, з боку будь-яких третіх осіб допускається виключно у випадку:

- якщо такий доступ прямо передбачений чинним законодавством України;
- якщо право на отримання такого доступу визначене за рішенням суду, ухваленим відповідно до чинного законодавства України, яке набрало законної сили;
- якщо право на отримання такого доступу визначене за рішенням Голови Фонду та/або уповноваженої ним особи, яке ґрунтується на положеннях чинного законодавства України;
- якщо отримання такого доступу зумовлено крайньою необхідністю, у тому числі ліквідацією та/або запобіганню виникнення негативних наслідків надзвичайних ситуацій природного, техногенного, воєнного чи будь-якого іншого характеру тощо.

4.1.2. Інформація, закріплена **в електронній формі**, може зберігатись Фондом на матеріальних носіях та/або у "хмарних" сховищах, та/або у будь-яких інших віртуальних носіях інформації.

Використання "хмарних" сховищ та/або інших віртуальних носіїв інформації, яка знаходиться у володінні Фонду, здійснюється останнім з урахуванням правил та умов, визначених власниками та/або адміністраторами відповідних інформаційних сервісів.

Географічне розташування "хмарних" сховищ та/або інших віртуальних носіїв інформації, яка знаходиться у володінні Фонду, фіксується Головою Фонду та/або уповноваженою ним особою, та/або Допоміжним органом, та/або Відповідальною особою.

Структурування "хмарних" сховищ та/або інших віртуальних носіїв інформації, яка знаходиться у володінні Фонду, здійснюється за рішенням Голови Фонду з урахуванням:

- максимально допустимого вмісту об'єму завантаження даних, передбачених умовами безоплатного/платного використання віртуального носія інформації;
- змісту та характеру інформації, яка зберігається/має зберігатись Фондом в електронній формі;
- кількості благодійних проєктів/програм, у межах яких здійснюються операції з використання інформації Фонду;
- вимог грантодавців (донорів) Фонду у межах реалізації окремих благодійних проєктів/програм;
- інших факторів, які впливають на визначення ефективності зберігання інформації, володільцем якої є Фонд, у межах виконання ним завдань статутної (благодійної) діяльності.

Кожна структурна одиниця “хмарного” сховища та/або інших віртуальних носіїв інформації, яка знаходиться у володінні Фонду (папка, розділ, підрозділ тощо) має бути забезпечена всіма доступними та практично необхідними засобами захисту, визначеними у п. 3.1. Політики.

Доступ до інформації, закріпленої **в електронній формі,** надається учасникам, працівникам, волонтерам та/або контрагентам Фонду на підставах, вказаних, зокрема у п. 4.1. Політики.

У залежності від обсягу операцій. які можуть бути здійснені з інформацією Фонду в електронній формі, доступ до неї поділяється на три рівні:
- **повний доступ** - дозволяє учасникам, працівникам, волонтерам та/або контрагентам Фонду здійснювати будь-які операції з інформацією в електронній формі, у тому числі її видалення;
- **частковий доступ** - дозволяє учасникам, працівникам, волонтерам та/або контрагентам Фонду здійснювати окремо визначену частину операцій з інформацією в електронній формі без права на її видалення;
- **обмежений доступ** - дозволяє учасникам, працівникам, волонтерам та/або контрагентам Фонду ознайомитись зі змістом інформації в електронній формі без можливості здійснення будь-яких операцій з нею, у тому числі операції видалення інформації.

Визначення **рівнів доступу** до “хмарних” сховищ, та/або будь-яких інших віртуальних носіїв інформації в електронній формі, володільцем якої є Фонд, для учасників, працівників, волонтерів, контрагентів Фонду здійснюється Головою Фонду та/або уповноваженою ним особою, та/або Допоміжним органом, та/або Відповідальною особою у порядку, встановленому Головою Фонду.

4.2. Надання доступу до інформаційних ресурсів Фонду, які використовуються **у межах комунікації на внутрішньому рівні**, здійснюється з дотриманням положень цієї Політики для всіх учасників, працівників, волонтерів та/або контрагентів Фонду, залучених до участі у виконанні завдань його статутної (благодійної) діяльності, якщо інше не визначено за рішенням Голови Фонду.

Надання доступу до інформаційних ресурсів Фонду, які використовуються **у межах комунікації на зовнішньому рівні**, здійснюється з дотриманням положень цієї Політики для тих учасників, працівників, волонтерів та/або контрагентів Фонду, до змісту та/або обсягу обов’язків яких входить здійснення операцій з інформацією, володільцем якої є Фонд, з використанням зазначених ресурсів за цільовим призначенням (опублікування, редагування, видалення інформації тощо), якщо інше не визначено за рішенням Голови Фонду.

4.3. Доступ до інформації, володільцем якої є Фонд, припиняється з моменту:
- закінчення трудових правовідносин - **для працівників Фонду**;
- закінчення цивільно-правових та/або господарських правовідносин - **для контрагентів Фонду**;
- закінчення провадження волонтерської діяльності від імені Фонду - **для волонтерів Фонду**;
- виходу або виключення з числа учасників Фонду - **для учасників Фонду**.

Після припинення доступу до інформації, володільцем якої є Фонд, учасники, працівники, волонтери, контрагенти Фонду за участі та/або з подальшим письмовим повідомленням Голови Фонду та/або уповноваженої ним особи, та/або представника Допоміжного органу, та/або Відповідальної особи зобов’язуються:
- передати всю інформацію (її примірники, копії примірників тощо), яка знаходилась у їх користуванні, Фонду;
- деактивувати свій доступ до всіх акаунтів, електронних кабінетів та/або інших засобів/інструментів використання інформації, володільцем якої є Фонду;
- за необхідності вчинити інші дії, визначені Головою Фонду та/або уповноваженою ним особою, та/або представником Допоміжного органу, та/або Відповідальною особою, необхідні для забезпечення дотримання належного рівня інформаційного захисту Фонду після завершення співпраці.

5. ПОРЯДОК ГЕНЕРАЦІЇ ТА ВИКОРИСТАННЯ ПАРОЛІВ

5.1. Одним із основним інженерно-технічних засобів захисту інформації, володільцем якої є Фонд, є **автентифікація користувачів за допомогою паролів.**

Паролі у розумінні цієї Політики поділяються на:
- **паролі для доступу до матеріальних носіїв інформації Фонду** (жорсткі диски, флеш-накопичувачі, компакт-диски тощо);
- **паролі для доступу до “хмарних” сховищ та/або інших віртуальних носіїв інформації Фонду** (Google Drive, OneDrive, Dropbox, Mega, Amazon Web Services тощо);
- **паролі для доступу до технічних засобів та/або програмно-технічного забезпечення** (технічні засоби - персональні комп’ютери, ноутбуки, планшети, смартфони тощо; програмно-технічне забезпечення - Windows, Linux, Ios, Android тощо);

- **паролі для доступу до інформаційних ресурсів Фонду** (акаунти у межах корпоративної пошти Фонду, акаунти для верифікації та/або реєстрації на платформах для участі у грантових конкурсах, веб-сайти, акаунти в соціальних мережах Instagram, Telegram, WhatsApp, Facebook тощо).

5.2. Паролі, вказані у п. 5.1. Політики, генеруються, змінюються, обліковуються та передаються Головою Фонду, та/або уповноваженою ним особою, та/або Допоміжним органом, та/або Відповідальною особою, якщо інше не визначено за рішенням Голови Фонду.

Облік та порядок зберігання паролів, визначених у цьому підпункті, здійснюється Головою Фонду, та/або уповноваженою ним особою, та/або Допоміжним органом, та/або Відповідальною особою у порядку, визначеному Головою Фонду, з дотриманням цієї Політики та чинного законодавства України.

Зберігання паролів, вказаних у цьому пункті, може здійснюватись з використанням спеціального програмного забезпечення (“LastPass”, “1Password” тощо).

Зміна паролів, вказаних у п. 5.1. Політики, здійснюється виключно Головою Фонду, та/або уповноваженою ним особою, та/або Допоміжним органом, та/або Відповідальною особою, у тому числі на підставі письмового звернення учасника, працівника, волонтера, контрагента Фонду, якщо інше не визначено за рішенням Голови Фонду.

5.3. Визначення Головою Фонду порядку генерування паролів, вказаних у п. 5.1. Політики, має, зокрема, містити умови щодо символів, які можуть використовуватись у паролі, мінімально допустиму кількість символів паролю, обмеження та заборони щодо використання окремих комбінацій паролів, порядок та особливості передачі згенерованих паролів тощо.

Паролі, зазначені у цьому пункті, не мають дублювати одне одного за жодних умов.

Під час передачі згенерованих паролів можуть використовуватись засоби шифрування, визначені Головою Фонду, та/або уповноваженою ним особою, та/або Допоміжним органом, та/або Відповідальною особою.

Забороняється передача паролів, зазначених у цьому пункті, з використанням незахищених каналів інформації, зокрема загально доступних мереж Wi-Fi, та/або під час знаходження у громадських місцях, у межах яких існує ризик неконтрольованого візуального спостереження з боку третіх осіб.

Використання програмно-технічного забезпечення та/або матеріальних носіїв інформації та/або “хмарних” сховищ, та/або будь-яких інших віртуальних носіїв інформації, правила/умови створення паролів у межах яких не відповідають тим, які визначені цим пунктом, з метою зберігання інформації, володільцем якої є Фонд, не допускається.

5.4. Учасники, працівники, волонтери, контрагенти Фонду самостійно несуть відповідальність за збереження отриманих ними паролів та вжиття заходів щодо протидії їх несанкціонованому отриманню з боку третіх осіб.

Учасники, працівники, волонтери та/або контрагенти Фонду можуть звернутись з використанням будь-яких доступних засобів зв’язку до Голови Фонду та/або уповноваженої ним особи, та/або Допоміжного органу, та/або Відповідальної особи для отримання роз’яснень та/або рекомендацій стосовно зберігання та/або передачі паролів, вказаних у п. 5.1. Політики.

Відповідь на вказані у цьому пункті звернення надається не пізніше ____ робочих днів з моменту їх отримання.

6. ПОРЯДОК ВИКОРИСТАННЯ ТЕХНІЧНИХ ЗАСОБІВ, ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ТА ІНФОРМАЦІЙНИХ РЕСУРСІВ ФОНДУ

6.1. Збір, обробка, зберігання та/або інші операції з інформацією, необхідною для належного виконання завдань статутної (благодійної) діяльності Фонду та/або яка знаходиться у володінні Фонду, здійснюється з використанням технічних засобів, які знаходяться у власності та/або користуванні Фонду.

Фонд забезпечує придбання та утримання технічних засобів, необхідних для виконання завдань його статутної (благодійної) діяльності, які відповідають вимогам міжнародних та національних технічних норм і стандартів.

6.2. Учасники, працівники, волонтери та/або контрагенти Фонду виконують свої статутні/трудові/цивільні/господарські/волонтерські обов’язки у межах взяття участі у провадження статутної (благодійної) діяльності Фонду з використанням технічних засобів Фонду, які знаходяться у власності Фонду, якщо інше не визначено:

- за рішенням Виконавчого директора Фонду;

- умовами трудових, цивільно-правових, господарських договорів, у тому числі договорів з ФОП/самозайнятими особами, договорів про провадження волонтерської діяльності.

6.2.1. Загальний порядок, строки та інші особливості процесу надання технічних засобів Фондом у користування особам, вказаним у п. 6.2. Політики, визначається:
- за рішенням Виконавчого директора Фонду;
- положеннями відповідних договорів, укладених між вказаними особами та Фондом.

Підставою для передачі Фондом технічних засобів особам, вказаним у п. 6.2. Політики, є відповідний **наказ Голови Фонду,** а наявність факту такої передачі фіксується в **Акті приймання-передачі матеріальних цінностей** (далі - Акт).

Акти виступають невід'ємними додатками до договорів між волонтерами та/або контрагентами, вказаним у п. 6.2. Політики, та Фондом.

6.2.2. Порядок надання технічних засобів Фонду його працівниками, які виконують свої трудові обов'язки у межах надомної та/або дистанційної роботи, визначається положеннями укладених з ними трудових договорів та нормами чинного трудового законодавства України.

Із працівником Фонду може бути укладений Договір про повну матеріальну відповідальність, включивши до його посадових інструкцій обов'язки щодо збереження наданого йому майна.

6.3. Учасники, працівники, волонтери та/або контрагенти Фонду отримують технічні засоби, а також паролі для користування ними, згенеровані з урахуванням положень Розділу 5 Політики, якщо інше не визначено за рішенням Голови Фонду.

Використання технічних засобів Фонду у межах виконання особами, вказаними у цьому пункті, завдань статутної (благодійної) діяльності Фонду без встановленого паролю для користування вказаними засобами не допускається.

6.4. У випадку виявлення працівником, волонтером та/або контрагентом наявності на технічному носії Фонду, отриманому ним для виконання своїх професійних, службових чи трудових обов'язків, інформації, яка виступає предметом захисту цієї Політики та була створена до моменту отримання ним технічного засобу, він невідкладно має письмово повідомити про це Голову Фонду, та/або уповноважену ним особою, та/або Допоміжний орган, та/або Відповідальну особу для вирішення питань, пов'язаних з передачею/подальшим зберіганням вказаної інформації.

6.5. Учасники, працівники, волонтери, контрагенти Фонду під час здійснення обробки інформації, володільцем якої є Фонд, мають використовувати всі доступні та практично ефективні засоби захисту, які встановлені на технічних засобах та/або виступають невід'ємною частиною їх програмного забезпечення.

Особи, зазначені у цьому пункті, можуть використовувати засоби шифрування інформації з метою запобігання вчиненню будь-яких несанкціонованих дій з боку третіх осіб, у тому числі учасників, працівників, волонтерів та/або контрагентів Фонду, щодо інформації, використання якої здійснюється у межах виконання професійних, службових, трудових та/або інших обов'язків, якщо:
- вони вважають, що таке шифрування підвищує рівень захисту інформації, володільцем якої є Фонд, за умови, що такі заходи не призведуть до непередбачуваної втрати інформації та/або несанкціонованих дій з нею з боку третіх осіб;

*Примітка: запобігання непередбачуваній втраті інформації та/або несанкціонованих дій з нею з боку третіх осіб здійснюється шляхом забезпечення **контрольованості процесів шифрування** (наприклад, відсутність доступу до шифрувального програмного забезпечення третіх осіб, завчасне надання засобів дешифрування Голові Фонду та/або іншій уповноваженій особі, зберігання засобів дешифрування у спосіб, який перешкоджає їх знищенню/втраті/пошкодженню тощо).*
- щодо цього було прийнято відповідне рішення Виконавчого директора Фонду;
- положення грантового договору (контракту) закріплюють необхідність та/або чіткий порядок використання засобів шифрування інформації Фондом під час реалізації його окремого благодійного проєкту.

Використання засобів резервного копіювання даних здійснюється особами, зазначені у цьому пункті, у межах та порядку, визначених відповідно до цієї Політики, з метою запобігання повній або частковій втраті інформації, володільцем якої є Фонд.

6.6. Повернення технічних засобів Фонду учасниками, працівниками, волонтерами та/або контрагентами Фонду після завершення виконання ними обов'язків, пов'язаних з використанням інформації, володільцем якої є Фонд, та/або співпраці з Фондом у цілому, здійснюється на підставі Акту.

6.7. Учасники, працівники, волонтери, контрагенти Фонду під час здійснення обробки інформації, володільцем якої є Фонд, мають використовувати виключно **ліцензійне програмне забезпечення**, придбання якого забезпечується Фондом.

Програмне забезпечення має своєчасно оновлюватись користувачами технічних засобів Фонду для підтримки актуальності їх функціоналу, зокрема у частині захисту цифрових даних.

Особи, зазначені у цьому пункті, зобов'язані самостійно слідкувати за налаштуванням та оновленням антивірусного програмного забезпечення у межах всього строку використання технічних засобів Фонду.

Відключення та/або видалення антивірусного програмного забезпечення без отримання попереднього дозволу Голови Фонду, та/або уповноваженої ним особи, та/або Допоміжного органу, та/або Відповідальної особи не допускається.

У випадку, якщо антивірусне програмне забезпечення призводить до некоректної роботи технічного засобу та/або звужує можливість його належного використання, учасники, працівники, волонтери, контрагенти Фонду невідкладно повідомляють про відповідні факти Голову Фонду, та/або уповноважену ним особою, та/або Допоміжний орган, та/або Відповідальну особу для вирішення відповідних питань.

Використання та налаштування брандмауера з метою запобігання проникненню в інформаційну систему Фонду шкідливих програм, вірусів тощо та зменшення ризиків вчинення несанкціонованих операцій з інформацією, володільцем якої є Фонд, здійснюється особами, зазначеними у цьому пункті, відповідно до вимог Голови Фонду, та/або уповноваженої ним особи, та/або Допоміжного органу, та/або Відповідальної особи.

6.8. У випадку втрати технічного засобу Фонду учасники, працівники, волонтери, контрагенти Фонду мають невідкладно у письмовій формі повідомити Голову Фонду, та/або уповноважену ним особу, та/або Допоміжний орган, та/або Відповідальну особу.

У випадку втрати технічного засобу Фонду особи, зазначені у цьому пункті, зобов’язані, зокрема, скористатись спеціалізованим програмним забезпечення для запобігання витоку інформації, яка належить Фонду, шляхом її видалення, блокування технічного пристрою у цілому тощо у віддаленому режимі.

6.9. Інформаційні ресурси Фонду використовуються учасниками, працівниками, волонтерами, контрагентами Фонду з дотриманням заходів захисту інформації, володільцем якої є Фонд, зокрема, але не виключно автентифікації користувачів, у тому числі двофакторної, застосування резервного копіювання даних, а також інших заходів, визначених за рішенням Голови Фонду.

Використання інформаційних ресурсів Фонду здійснюється виключно з використанням технічних засобів Фонду та/або акаунтів, автентифікація яких здійснюється за двофакторною принципом з використанням корпоративної пошти Фонду. якщо не визначено за рішенням Голови Фонду.

Видалення інформації, яка зберігається у межах інформаційних ресурсів Фонду, здійснюється за рішенням Голови Фонду, та/або уповноваженої ним особи, та/або Допоміжного органу, та/або Відповідальної особи у разі, зокрема:

- втрати інформацією актуальності;
- завершення реалізації благодійного проєкту/програми, у межах яких використовувалась та чи інша інформація;
- необхідності запобігання несанкціонованим операціям з інформацією з боку третіх осіб;
- в інших випадках з урахуванням інтересів статутної діяльності Фонду.

Автоматичне видалення інформації, яка зберігається у межах інформаційних ресурсів Фонду, допускається виключно у випадках, визначених за рішенням Голови Фонду.

7. МОНІТОРИНГ ДОТРИМАННЯ ПОЛІТИКИ. ПОРЯДОК ВИЯВЛЕННЯ ТА РЕАГУВАННЯ НА ПОРУШЕННЯ ПОЛІТИКИ

7.1. Голова Фонду та/або уповноважена ним особа, та/або Допоміжний орган, та/або Відповідальна особа здійснює періодичний моніторинг результатів практичної реалізації цієї Політики шляхом, зокрема:

- отримання звітів від учасників, працівників, волонтерів та/або контрагентів Фонду про стан дотримання ними положень Політики;
- перевірку застосування дієвості інженерно-технічних засобів захисту інформації, володільцем якої є Фонд, у тому числі за участі третіх осіб (спеціалістів, експертів у сфері технологій захисту інформації, кібербезпеки);

- перевірку належності оформлення документів, пов'язаних з дотриманням положень Політики (наявність Згод-повідомлень, облік запитів на отримання інформації та результати їх обробки, положення договорів, укладених Фондом, у частині захисту інформації тощо);
- вжиття інших моніторингових заходів, визначених Головою Фонду та/або уповноваженою ним особа, та/або Допоміжним органом, та/або Відповідальною особою.

У випадку утворення Допоміжного органу або призначення Відповідальної особи останні мають подавати на запит Голови Фонду комплексні звіти про результати дотримання Політики та рівень захисту інформації, володільцем якої є Фонд, у певний проміжок часу.

Порядок проведення моніторингових заходів, вказаних у цьому пункті, визначається за рішенням Голови Фонду.

7.2. З метою підтримки належного рівня знань серед учасників, працівників, волонтерів та контрагентів Фонду, які беруть безпосередню участь у виконанні завдань статутної (благодійної) діяльності Фонду, у сфері технологій захисту інформації та кібербезпеки, Фонд сприяє проведенню періодичних контрольних, інформаційних та/або освітніх заходів серед вказаних осіб (далі - Періодичні заходи).

До таких Періодичних заходів відносяться, зокрема:
- тематичні тренінги, заходи неформальної освіти, вебінари тощо;
- проходження періодичних оцінювань та/або тестувань;
- залучення зовнішніх спеціалістів та експертів у сфері технологій захисту інформації та кібербезпеки;
- будь-які інші заходи, спрямовані на виконання завдань цієї Політики.

Участь у Періодичних заходах, організованих Фондом, є обов'язковою, якщо інше не визначено за рішенням Голови Фонду.

7.3. Факти порушень пололжень цієї Політики повинні бути документально зафіксовані Головою Фонду та/або уповноваженою ним особа, та/або Допоміжним органом, та/або Відповідальною особою.

Повідомлення про факти порушення Політики (далі - Повідомлення) може бути здійснено будь-яким учасником, працівником, волонтером, контрагентом, бенефіціаром Фонду та/або будь-якою третьою особою у разі, якщо вони стали їм відомі як внаслідок особистого спостереження/виявлення, так і зі сторонніх джерел.
Повідомлення має бути здійснено у письмовій формі, якщо інше не визначено Головою Фонду.

Реєстрація Повідомлень здійснюється у письмовій та/або електронній формі у Журналі реєстрації повідомлень, порядок створення та ведення якого визначається Головою Фонду шляхом видання відповідного наказу.

7.4. Голова Фонду та/або уповноважена ним особа, та/або Допоміжний орган, та/або Відповідальна особа має вжити всіх можливих, необхідних та доступних дій для:
- припинити порушення Політики у разі, якщо воно триває;
- встановити особу, винну у вчиненні порушення цієї Політики;
- встановити суб'єктів, права, свободи та/або законні інтереси яких порушені та/або знаходяться під реальною загрозою порушення внаслідок недотримання цієї Політики;
- ініціювати притягнення особи, винної у вчиненні порушення цієї Політики, до юридичної відповідальності;
- сприяти відновленню, наскільки це можливо, правового становища суб'єктів, права, свободи та/або законні інтереси яких були порушені внаслідок недотримання цієї Політики;
- переконатись у відсутності будь-яких загроз для комплексної системи захисту інформації, володільцем якої є Фонд, внаслідок порушення цієї Політики.

Строк розгляду Повідомлень та вчинення дій, вказаних у цьому пункті, не перевищує ____ робочих днів з моменту отримання та реєстрації відповідного Повідомлення.
У випадку необхідності, коли Голова Фонду та/або уповноважена ним особа, та/або Допоміжний орган, та/або Відповідальна особа потребує додаткового часу для належного здійснення своїх повноважень, цей строк може бути продовжено за рішенням Голови Фонду (у випадку, якщо він виступає Відповідальною особою - Загальних зборів Фонду) на строк, необхідний для такого здійснення, але не більше, ніж на ____ робочих днів.

7.5. Особи, що мають доступ до інформації, володільцем якої є Фонд, у тому числі, здійснюють її обробку, у разі порушення ними вимог цієї Політики та/або вимог чинного законодавства України у сфері захисту інформації несуть дисциплінарну, цивільну, адміністративну, кримінальну відповідальність згідно із чинним законодавством України.

7.6. У випадку виявлення у фактах порушень Політики ознак вчинення адміністративного та/або кримінального правопорушення Голова Фонду та/або уповноважена ним особа, та/або Допоміжний орган, та/або Відповідальна

особа за необхідності має право повідомити про це правоохоронні органи та/або уповноважені органи державної влади.

7.7. У випадку, коли дії/бездіяльність, рішення учасника, працівника, волонтера, контрагента Фонду призвели до порушення вимог законодавства України у сфері захисту інформації, внаслідок чого Фонд зобов'язаний відшкодувати збитки та/або іншу шкоду, завдану третім особам, такі учасники, працівники, волонтери та/або контрагенти Фонду мають відшкодувати вказані суми на користь Фонду у порядку регресу.