ЗАТВЕРДЖУЮ
Голова ГО «Проти Корупції»
_____ Путря Ю.М.
«03» грудня 2024 р.

ПОЛІТИКА ЦИФРОВОЇ БЕЗПЕКИ ГРОМАДСЬКОЇ ОРГАНІЗАЦІЇ «ПРОТИ КОРУПЦІЇ»

м. Корсунь-Шевченківський, Черкаська область

Метою цієї Політики є забезпечення високого рівня безпеки, конфіденційності, цілісності та доступності інформації ГО «Проти Корупції» та її учасників. Ця Політика створена з метою виявлення, запобігання та мінімізації ризиків, пов'язаних з використанням інформаційних ресурсів.

Захист інформації: метою є забезпечення захисту конфіденційної інформації організації, включно з персональними даними працівників, волонтерів, бенефіціарів і партнерів, а також конфіденційних документів (грантових угод, фінансових звітів, аналітики).

Запобігання загрозам: Політика призначена для запобігання виникненню ризиків, пов'язаних із вірусами, шахрайством, атаками ззовні чи всередині організації, у тому числі цілеспрямованими атаками з боку російських хакерських груп та проросійських акторів у зв'язку з антикорупційною діяльністю ГО.

Забезпечення доступності: метою є забезпечення безперебійної доступності інформаційних ресурсів, необхідних для нормальної діяльності організації в умовах війни, відключень електроенергії, потенційних кібератак на критичну інфраструктуру.

Ефективне використання технологій: Політика спрямована на забезпечення безпечного та ефективного використання інформаційних технологій, зокрема системи обліку Odoo, платформи DREAM, аналітичних систем BRP.

Дотримання нормативів: метою є забезпечення відповідності організації всім законодавчим та регуляторним вимогам, що стосуються цифрової безпеки та захисту персональних даних (Закон України «Про захист персональних даних», вимоги GDPR — там, де застосовно, вимоги донорів).

Свідомість і навчання: Політика спрямована на підвищення рівня свідомості та навичок з цифрової безпеки серед усіх користувачів.

Швидка відновлюваність: метою є забезпечення можливості швидкого та ефективного відновлення робочих процесів у разі інциденту або аварії.

Цілі політики

- **Захист інформації** — забезпечити конфіденційність персональних даних працівників, волонтерів, бенефіціарів та конфіденційної інформації організації.
- **Проактивний захист** — передбачити та запобігти можливим атакам, вірусам та іншим загрозам.
- **Швидке відновлення** — забезпечити можливість швидкого та ефективного відновлення інформаційних ресурсів після інциденту чи аварії.

Сфера дії

Ця Політика поширюється на всіх працівників, волонтерів, підрядників, партнерів та інших осіб, які мають доступ до інформаційних ресурсів, комп'ютерної техніки та ЛКМ ГО «Проти Корупції».

Визначення та абревіатури

- ГО — громадська організація
- ІТ — інформаційні технології
- ПЗ — програмне забезпечення
- ЛКМ — локальні комунікаційні мережі
- 2FA — багатофакторна автентифікація
- VPN — віртуальна приватна мережа

Системне та програмне забезпечення

Усі системи та програмне забезпечення повинні бути оновлюваними до останніх версій з урахуванням патчів безпеки. Перед встановленням нового програмного забезпечення слід отримати схвалення від відповідального за ІТ-безпеку особи, призначеної Головою організації.

Системне ПЗ. Забезпечує функціонування обладнання та зв'язок між обладнанням і стандартним та прикладним ПЗ. Комп'ютери організації можуть мати лише ліцензійні версії операційних систем (Windows 10/11, macOS, Linux — на вибір користувача, у межах бюджету). Для функціонування периферійного обладнання дозволено використовувати драйвери лише із сайту виробника.

Стандартне ПЗ. Забезпечує безпеку роботи комп'ютера та роботу з документами. Для виконання робочих цілей на робочих комп'ютерах організації встановлюються ліцензійні програми: пакет офісних програм (Microsoft 365, LibreOffice або Google Workspace), архіватор (7-Zip, WinRAR), антивірус (Microsoft Defender або еквівалент), Signal/захищений месенджер, менеджер паролів (Bitwarden, 1Password або еквівалент).

Створення нового користувача

1. Отримати електронною поштою інформацію про нового працівника, волонтера або підрядника від менеджерки проєктів (Карина Арбузова) або особи, відповідальної за кадрові питання: прізвище, ім'я та по батькові; особиста електронна пошта; доступи до груп/сервісів організації.

2. Створення облікового запису, додавання його до робочих груп і надсилання інструкції для входження. При створенні обов'язково встановлюється унікальний та складний пароль, який змінюється не рідше ніж кожні 90 днів. Особа, відповідальна за ІТ, надає лише необхідні права доступу за принципом мінімальних привілеїв.

3. Придбати та/або підготувати запитане обладнання для нового працівника.

4. Ознайомити нового працівника з цією Політикою під підпис, перевірити розуміння, надати необхідну інформацію про IT-інфраструктуру.

5. Видати запитане обладнання.

6. Допомогти новому користувачу змінити пароль і налаштувати багаторівневу автентифікацію (2FA).

7. Допомогти підключитися до локальної комп'ютерної мережі або Wi-Fi (з використанням WPA2/WPA3, без публічних відкритих мереж).

Видалення користувача

1. Отримати електронною поштою інформацію про завершення співпраці з працівником, волонтером або підрядником.
2. Негайно заблокувати обліковий запис і анулювати всі права доступу.
3. Повернути все обладнання відповідальному за IT.
4. Перевірити комплектність обладнання, стерти або зашифрувати особисті дані.
5. Оновити паролі до спільних облікових записів, до яких мала доступ ця особа.

Використання обладнання

Кожен користувач несе персональну відповідальність за цілісність та працездатність виданого обладнання. Обладнання встановлюється та налаштовується з урахуванням цієї Політики та найновіших стандартів безпеки. Регулярно (не рідше 1 разу на місяць) проводиться аудит стану та безпеки обладнання.

Доступ до ресурсів IT

Доступ до ресурсів IT суворо регламентований та захищений відповідними ідентифікаторами й паролями, які знає лише користувач. Кожен користувач має тільки необхідний мінімум прав доступу для виконання своїх обов'язків. Доступ до критичних сервісів (банківські системи, бухгалтерські системи, Odoo, ЕЦП) обмежений відповідальними особами (у першу чергу — фінансовий менеджер Віра Петренко та Голова організації).

Підключення зовнішніх пристроїв для зберігання даних

Забороняється використання власних зовнішніх пристроїв для зберігання даних без попереднього схвалення особи, відповідальної за IT-безпеку. Дозволяється підключати лише службові, перевірені антивірусом зовнішні пристрої (USB-флеш, SD-картки, зовнішні жорсткі диски).

Безпека комп'ютера, ПЗ і ЛКМ

Категорично забороняється:

1. Повідомляти будь-кому свої ідентифікатори та паролі доступу. Паролі відомі лише користувачу. Співробітники IT можуть лише допомогти користувачу змінити їх.

2. Залишати відкритий для доступу комп'ютер без нагляду на час понад 10 хвилин — обов'язково використовуйте блокування екрана з паролем (Win+L або Ctrl+Cmd+Q).
3. Залишати ввімкнений комп'ютер після робочого часу без потреби.
4. Дозволяти стороннім особам користуватися ресурсами IT.
5. Використовувати комп'ютер без антивірусу або відключати автоматичне оновлення антивірусної програми.
6. Вносити зміни в системні файли та конфігурацію комп'ютера, оскільки це може призвести до порушення функціонування системи.
7. Встановлювати будь-яке несанкціоноване програмне забезпечення (у тому числі ігри, піратські версії). Виявлені неавторизовані програми будуть негайно та без попередження видалені.
8. Використовувати службову електронну пошту та Інтернет для доступу до інформації, не пов'язаної зі службовими обов'язками.
9. Розповсюджувати інформацію, яка може бути використана хакерами та зловмисниками (особиста, фінансова, безпекова інформація).
10. Заходити на підозрілі й незахищені сайти без HTTPS, переходити за невідомими або рекламними посиланнями, відкривати вкладення від невідомих відправників.
11. Користуватися незахищеними з'єднаннями для передачі чутливої інформації в мережі. У виїздах або в громадських Wi-Fi мережах — обов'язково використовувати VPN.
12. Користуватися незахищеними месенджерами (наприклад, Facebook Messenger, Viber, Telegram) для передачі чутливої інформації. Для конфіденційної комунікації — використовувати Signal.
13. Публікувати в соціальних мережах геолокаційні дані, фото робочих документів, обличчя партнерів у громадах без їх згоди.

У разі систематичного порушення цих правил особа, відповідальна за IT, має право відключати користувачів від ресурсів IT до з'ясування обставин Головою організації.

Правила створення паролю

1. Пароль повинен містити мінімум **12 символів** (рекомендовано 16+).
2. Пароль повинен містити щонайменше 3 з 4 класів символів:
   - латинські великі літери A-Z;
   - латинські малі літери a-z;
   - цифри 0-9;
   - символи ~ ! @ # $ % ^ & * ( ) - _ + = { } [ ] : " ' < > ? , .
3. Паролі оновлюються не рідше ніж кожні 90 днів.
4. Пароль від облікового запису обов'язково прив'язується до телефонного номера або застосунку 2FA (Google Authenticator, Authy) для багатофакторної автентифікації.
5. Забороняється повторне використання одного пароля для різних сервісів. Використовувати менеджер паролів.
6. Забороняється зберігати паролі у відкритому вигляді (стікери на моніторі, файли на робочому столі).

Доступ до інтернет-ресурсів організації

Доступ до інтернет-ресурсів організації (сайт protucor.com, соціальні мережі, аналітичні сервіси, платформа DREAM, BRP тощо) надається за погодженням Голови організації або менеджерки проєктів письмовим запитом до IT-спеціаліста.

Бекап інформації

Необхідно **щотижня** робити резервне копіювання інформації на зовнішні пристрої та/або в захищене хмарне сховище (з шифруванням) і зберігати їх у безпечному місці окремо від основного комп'ютера. **Щоквартально** проводяться тести відновлення даних для переконання в їхній доступності у випадку інциденту.

Критичні дані (фінансова документація, грантові угоди, персональні дані команди) зберігаються з подвійним резервуванням.

Реагування на інциденти

У разі виявлення інциденту (втрата пристрою, підозра на злом облікового запису, отримання фішингового листа, крадіжка) співробітник негайно повідомляє менеджерку проєктів та Голову організації. Особа, відповідальна за IT, координує реагування: зміна паролів, блокування скомпрометованих облікових записів, повідомлення партнерів, за необхідності — CERT-UA та поліції.

Ця Політика цифрової безпеки є обов'язковою для всіх працівників, волонтерів, підрядників та осіб, які мають доступ до інформаційних ресурсів ГО «Проти Корупції». Невиконання Політики може призвести до санкцій, включно з припиненням трудових/договірних відносин або правовою відповідальністю.