МГО “ДієМолодь”
Широка 4
ngodiemolod@gmail.com
+380 93 160 33 80

ПОЛОЖЕННЯ

ПРО ІНФОРМАЦІЙНУ БЕЗПЕКУ

Версія документа: 1.0
Дата набрання чинності: «26» серпня 2026 року
Дата наступного перегляду (орієнтовно): «20» червня 2029 року

ЗАТВЕРДЖЕНО
Рішенням Правління Громадської організації «Молодіжна організація «ДієМолодь»

26.08.26 _____ _____
дата підпис місце для печатки

1. ЗАГАЛЬНІ ПОЛОЖЕННЯ

1.1. Це Положення визначає основні принципи, завдання та заходи щодо забезпечення інформаційної безпеки у Громадській організації «Молодіжна організація «ДієМолодь» (далі – Організація).

1.2. Метою цього Положення є встановлення єдиних організаційних, технічних та адміністративних вимог щодо забезпечення інформаційної безпеки Організації, захисту інформаційних активів, персональних даних, цифрових сервісів та інформаційних систем від випадкових або навмисних загроз, а також мінімізація ризиків втрати, пошкодження, несанкціонованого доступу, розголошення чи неправомірного використання інформації.

1.3. Положення є обов'язковим для виконання всіма співробітниками, волонтерами та іншими особами, які мають доступ до інформаційних ресурсів Організації.

2. ТЕРМІНИ ТА ВИЗНАЧЕННЯ

2.1. Інформаційна безпека - стан захищеності інформаційних ресурсів від внутрішніх та зовнішніх загроз.

2.2. Інформаційні ресурси - сукупність даних, інформаційних систем, мереж та засобів їх забезпечення, що належать або використовуються Організацією.

2.3. Несанкціонований доступ - доступ до інформаційних ресурсів без відповідного дозволу.

2.4. Персональні дані - будь-яка інформація, що стосується ідентифікованої або такої, що може бути ідентифікована, фізичної особи.

2.5. Робочі пристрої - комп'ютери, ноутбуки, мобільні телефони, планшети та інші електронні пристрої, що використовуються для виконання робочих завдань.

2.6. Інцидент інформаційної безпеки - будь-яка подія або сукупність подій, що призвела або може призвести до порушення конфіденційності, цілісності чи доступності інформації або інформаційних ресурсів Організації.

2.7. Конфіденційна інформація - інформація, доступ до якої обмежений законодавством України, внутрішніми документами Організації або умовами договорів із партнерами, донорами чи іншими особами.

3. ПРИНЦИПИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

3.1. Конфіденційність - забезпечення доступу до інформації лише уповноваженим особам.

3.2. Цілісність - захист інформації від несанкціонованої модифікації або знищення.

3.3. Доступність - забезпечення своєчасного та безперешкодного доступу до інформації для уповноважених користувачів.

3.4. Організація застосовує принцип мінімально необхідного доступу, відповідно до якого кожна особа отримує доступ лише до тих інформаційних ресурсів, які необхідні їй для виконання службових, договірних або волонтерських обов'язків.

4. ОСНОВНІ ЗАВДАННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

4.1. Розробка та впровадження політик і процедур захисту інформаційних ресурсів.

4.2. Навчання та підвищення обізнаності співробітників щодо питань інформаційної безпеки.

4.3. Моніторинг та аудит інформаційних систем для виявлення та запобігання потенційним загрозам.

4.4. Захист персональних даних співробітників, волонтерів та бенефіціарів від розголошення, втрати або несанкціонованого використання.

4.5. Розробка планів реагування на інциденти, пов'язані з інформаційною безпекою.

4.6. Організація здійснює періодичну оцінку ризиків інформаційної безпеки та впроваджує заходи щодо їх мінімізації з урахуванням характеру своєї діяльності та наявних інформаційних ресурсів.

5. ОБОВ'ЯЗКИ СПІВРОБІТНИКІВ ТА ВОЛОНТЕРІВ

5.1. Дотримуватися встановлених політик та процедур інформаційної безпеки.

5.2. Невідкладно виконувати вимоги цього Положення щодо повідомлення про інциденти інформаційної безпеки.

5.3. Забезпечувати конфіденційність інформації, до якої вони мають доступ, і не розголошувати її без відповідного дозволу.

5.4. Використовувати надійні паролі для доступу до інформаційних систем та пристроїв.

5.5. Не використовувати робочі пристрої для особистих цілей без дозволу керівництва.

5.6. Захищати робочі пристрої від несанкціонованого доступу, зокрема використовуючи засоби шифрування, антивірусне програмне забезпечення та двофакторну аутентифікацію.

5.7. Не використовувати відкриті сервіси штучного інтелекту, особисті хмарні сховища чи інші сторонні цифрові сервіси для обробки або зберігання конфіденційної інформації, персональних даних або службових документів Організації без відповідного дозволу Голови Організації або іншої уповноваженої особи.

6. ТЕХНІЧНІ ЗАХОДИ ЗАХИСТУ

6.1. Використання сучасних засобів захисту інформації, таких як антивірусні програми, міжмережеві екрани та системи виявлення вторгнень.

6.2. Регулярне оновлення програмного забезпечення та встановлення патчів безпеки.

6.3. Організація забезпечує регулярне резервне копіювання критично важливої інформації із визначенням відповідальної особи, місця зберігання резервних копій та періодичності їх створення відповідно до внутрішніх процедур Організації.

6.4. Обмеження фізичного доступу до серверів та робочих пристроїв.

6.5. Використання шифрування для захисту конфіденційних даних.

7. ОРГАНІЗАЦІЙНІ ЗАХОДИ ЗАХИСТУ

7.1. Визначення Головою Організації відповідальної особи (або відповідальних осіб) за координацію заходів із забезпечення інформаційної безпеки залежно від організаційної структури та потреб Організації.

7.2. Проведення регулярних тренінгів та семінарів для підвищення обізнаності співробітників щодо інформаційної безпеки.

7.3. Розробка та впровадження процедур управління доступом до інформаційних ресурсів.

7.4. Регламентування використання особистих пристроїв для роботи.

8. ЗАХИСТ ДОСТУПУ ДО РЕСУРСІВ ОРГАНІЗАЦІЇ

8.1.Створення нового користувача.

8.1.1. Уповноважена особа Організації отримує необхідні дані для створення корпоративного облікового запису.

8.1.2. Ознайомити нового співробітника, учасника програми та проєкту з правилами даного Положення, перевірити, що новий співробітник, учасник програми та проєкту їх розуміє і дати йому необхідну інформацію про інфраструктуру ІТ.

8.1.3. Видати новому співробітнику, учаснику програми та проєкту запитане обладнання (за наявності).

8.1.4. Допомогти новому співробітнику, учаснику програми та проєкту змінити пароль облікового запису і налаштувати багаторівневу аутентифікацію.

8.1.5. Допомогти підключитися до локальної комп'ютерної мережі або Wi-Fi.

8.2. Видалення користувача.

8.2.1. Після отримання інформації про припинення трудових, цивільно-правових, волонтерських або інших відносин з особою, відповідальна особа забезпечує припинення або обмеження її доступу до інформаційних ресурсів Організації.

8.2.2. Облікові записи, корпоративна електронна пошта та інші засоби доступу до інформаційних ресурсів Організації блокуються або видаляються відповідно до внутрішніх процедур Організації.

8.2.3. Особа зобов'язана повернути Організації видане їй обладнання, носії інформації та інші матеріальні цінності, якщо вони були передані у користування.

8.2.4. Відповідальна особа перевіряє комплектність, технічний стан повернутого обладнання та, за потреби, забезпечує передачу інформації, що зберігалася на ньому, до відповідних інформаційних ресурсів Організації.

8.3. Використання обладнання.

Кожний Користувач несе персональну відповідальність за цілісність та працездатність виданого йому обладнання.

8.4. Доступ до ресурсів ІТ.

Доступ до ресурсів ІТ суворо регламентований та захищений відповідними ідентифікаторами та паролями, які знає тільки Користувач. Час доступу до ресурсів ІТ не обмежений, за випадком проведення встановлювальних, ремонтних або профілактичних робіт.

8.5. Підключення зовнішніх пристроїв для зберігання даних.

Дозволяється підключати до службових комп'ютерів/ноутбуків тільки перевірені антивірусом зовнішні пристрої для зберігання даних (USB флеш-пам'ять, картки пам'яті SD та інші, зовнішні жорсткі диски тощо).

8.6. Безпека комп'ютера/ноутбука, програмного забезпечення (ПЗ) і локальної комп'ютерної мережі (ЛКМ).

Для забезпечення безпеки комп'ютера, ПЗ і ЛКМ категорично забороняється:

8.6.1. Повідомляти будь-кому свої ідентифікатори та паролі доступу.

- Паролі доступу відомі тільки користувачу. Співробітники ІТ можуть тільки допомогти користувачу змінити їх;

- Співробітники ІТ не мають права повідомляти інформацію про облікові записи, адреси електронної пошти і т.і. інших користувачів.

8.6.2. Залишати відкритий для доступу комп'ютер без нагляду на час більше 10 хвилин - будь ласка використовуйте зберігач екрану з паролем.

8.6.3. Залишати включений комп'ютер після роботи - будь ласка вимикайте комп'ютер після закінчення робочого часу.

8.6.4. Дозволяти стороннім людям використовувати ресурси ІТ.

8.6.5. Використовувати комп'ютер без антивірусу.

8.6.6. Вносити зміни в системні файли та конфігурацію комп'ютера, так як це може призвести до порушення функціонування комп'ютера і ЛКМ в цілому.

8.6.7. Встановлювати як на локальні, так і на мережеві диски будь-яке програмне забезпечення (в т.ч. ігри). Виявлені неавторизовані програми будуть негайно та без попередження видалені.

8.6.8. Використовувати електронну пошту та мережу Інтернет для доступу до інформації не пов'язаної зі службовими обов'язками (ігри, музика і т.п.).

8.6.9. Розповсюджувати інформацію яка може бути використана хакерами та зловмисниками (особиста, фінансова інформація).

8.6.10. Не відвідувати підозрілі або потенційно небезпечні вебресурси та не переходити за сумнівними посиланнями з електронних листів, повідомлень або рекламних матеріалів.

8.6.11. Користуватись незахищеними з'єднаннями для передачі сенситивної інформації в мережі.

8.6.12. Не використовувати месенджери або інші засоби електронної комунікації, не погоджені Організацією, для передачі конфіденційної інформації чи персональних даних.

8.7. Правила створення паролю.

8.7.1. Пароль повинен містити мінімум 8 символів.

8.7.2. Пароль повинен містити в собі як мінімум 3 класи символів з наступних 4-х класів:

- Латинські великі літери A B C ... Z
- Латинські малі літери a b c ... z
- Цифри 012 …9
- Символи - !#S%^&*()_+-={3|[]1:; '<>?,.

8.7.3. Пароль від електронної адреси обов'язково потрібно закріплювати за телефонним номером, для подвійної аутентифікації.

8.8. Підключення до корпоративної мережі Wi-Fi здійснюється виключно із використанням параметрів доступу, визначених Організацією. Забороняється передавати паролі доступу до корпоративної мережі третім особам без дозволу відповідальної особи або Голови Організації.

8.9. Резервне копіювання інформації здійснюється відповідно до внутрішніх процедур Організації із забезпеченням належного захисту резервних копій від втрати, пошкодження або несанкціонованого доступу.

9. ВІДПОВІДАЛЬНІСТЬ ЗА ПОРУШЕННЯ

9.1. Особи, винні у порушенні вимог цього Положення, несуть відповідальність відповідно до чинного законодавства України та внутрішніх документів Організації.

9.2. У разі виявлення або виникнення підозри щодо інциденту інформаційної безпеки, порушення вимог цього Положення чи несанкціонованого доступу до інформаційних ресурсів Організації особа зобов'язана невідкладно повідомити про це свого безпосереднього керівника, Голову Організації або іншу визначену відповідальну особу.

9.3. У разі виявлення порушень інформаційної безпеки керівництво Організації може вживати заходів, включаючи обмеження доступу до інформаційних ресурсів, застосування дисциплінарних заходів або залучення правоохоронних органів.

10. ЗАКЛЮЧНІ ПОЛОЖЕННЯ

10.1. Це Положення набуває чинності з дня його затвердження наказом Голови Організації, якщо інше не визначено таким наказом.

10.2. Це Положення переглядається за потреби, але не рідше одного разу на три роки або у разі істотних змін законодавства України, організаційної структури, інформаційної інфраструктури чи після виникнення суттєвого інциденту інформаційної безпеки.

10.3. У питаннях, не врегульованих цим Положенням, Організація керується законодавством України, Статутом та іншими внутрішніми документами Організації.