Затверджено
Голова _____Є.Бєліцька
Прийнята «_23_» грудня 2019 року
Протокол № 2

ПОЛІТИКА КОНФІДЕНЦІЙНОСТІ ГРОМАДСЬКОЇ ОРГАНІЗАЦІЇ «ЦЕНТР РОЗВИТКУ ФІЛОЛОГІЇ»

КОНФІДЕНЦІЙНІСТЬ ДАНИХ - ЦЕ ЗАХИСТ ДАНИХ ВІД НЕНАВМИСНОГО, НЕЗАКОННОГО ЧИ НЕСАНКЦІОНОВАНОГО ДОСТУПУ, РОЗГОЛОШЕННЯ ЧИ КРАДІЖКИ.

Конфіденційність пов'язана з конфіденційністю інформації, включаючи дозволи на її перегляд, обмін та використання. Інформація, що викликає загрозу конфіденційності, може вважатися "публічною" або іншим чином не загрожувати, якщо вона потрапляє за межі передбачуваної аудиторії. Інформація, яка викликає загрозу конфіденційності, вважається таємною і повинна зберігатись у тіємниці, щоб запобігти крадіжці особистих даних, компрометації облікових записів та систем, пошкодженню права або репутації та іншим серйозним наслідкам.

При управлінні конфіденційністю даних враховуйте наступне:

- **Хто є адресантом інформації**
- **Чи мають нормативні акти чи контракти бути конфіденційними**
- **Чи можна використовувати дані за будь-яких умов**
- **Чи є дані чутливими за своєю природою і чи матимуть негативний вплив у разі їх розголошення**
- **Чи дані будуть цінними для тих, кому не дозволено їх мати (наприклад, хакерам)**

Керуючи конфіденційністю даних, дотримуйтесь цих вказівок:

1. **Шифруйте конфіденційні файли.**

Шифрування - це процес, який робить дані нечитабельними для всіх, крім тих, хто має відповідний пароль або ключ. Шифруючи конфіденційні файли

(наприклад, використовуючи файлові паролі), ви можете захистити їх від читання або використання тими, хто не має права робити це.

2. **Керуйте доступом до даних.**

Контроль конфіденційності здебільшого полягає у контролі над тим, хто має доступ до даних. Забезпечення того, що доступ дозволений і надається лише тим, хто має "потребу знати", значно сприяє обмеженню непотрібного впливу. Користувачі також повинні автентифікувати свій доступ надійними паролями та, де це можливо, двофакторною автентифікацією. Періодично переглядайте списки доступу та негайно відкликайте доступ, коли це більше не потрібно.

3. **Фізично захищайте пристрої та паперові документи.**

Контроль доступу до даних включає контроль доступу всіх видів, як цифрового, так і фізичного. Захистіть пристрої та паперові документи від неправильного використання або крадіжки, зберігаючи їх у заблокованих місцях. Ніколи не залишайте пристрої або конфіденційні документи без уваги у громадських місцях.

4. **Надійно утилізуйте дані, пристрої та паперові записи.**

Коли дані більше не потрібні для цілей Громадської організації, вони повинні бути належним чином утилізовані.

Конфіденційні дані, такі як номери соціального страхування, повинні бути надійно стерті, щоб не можна було їх відновити та зловживати ними.

Пристрої, які використовувались для цілей Громадської організації або які використовувались в інший спосіб для зберігання конфіденційної інформації, слід знищувати або надійно стирати, щоб переконатись, що їх попередній вміст не може бути відновлений та використаний неправильно.

Паперові документи, що містять конфіденційну інформацію, слід подрібнювати, а не скидати у смітник або урни для сміття.

5. **Керуйте збором даних.**

Збираючи конфіденційні дані, пам'ятайте, скільки даних насправді потрібно, і ретельно враховуйте конфіденційність та конфіденційність у процесі отримання. Уникайте отримання конфіденційних даних, якщо це не є абсолютно необхідним; один із найкращих способів зменшити ризик конфіденційності - це зменшення кількості конфіденційних даних, що збираються у першу чергу.

6. **Керуйте використанням даних.**

Ризик конфіденційності можна додатково зменшити, використовуючи конфіденційні дані лише за схваленням та за необхідності. Зловживання

конфіденційними даними порушує конфіденційність та конфіденційність цих даних та осіб чи груп, які вони представляють.

7. **Керуйте пристроями.**

Управління комп'ютером - це широка тема, яка включає багато важливих практик безпеки. Захистивши пристрої, ви також можете захистити дані, які вони містять. Дотримуйтесь елементарної гігієни кібербезпеки, використовуючи антивірусне програмне забезпечення, регулярно виправляючи програмне забезпечення, додатки з білого списку, використовуючи коди доступу до пристрою, призупиняючи неактивні сеанси, активуючи брандмауери та використовуючи шифрування всього диска.