БЛАГОДІЙНА ОРГАНІЗАЦІЯ «БЛАГОДІЙНИЙ ФОНД «СТАБІЛІЗЕЙШЕН СУППОРТ СЕРВІСЕЗ» CHARITABLE ORGANIZATION «CHARITY FOUNDATION «STABILIZATION SUPPORT SERVICES» 04053, Україна, м. Київ, вул. Січових Стрільців, 1-5
ЄДРПОУ 40567253, р/р 26008500242960 банк ПАТ «Креді Агріколь Банк», МФО 300614

Політика інформаційної безпеки Благодійної організації "Благодійний фонд "Стабілізейшен Суппорт Сервісез"

Інформація про документ	
Версія документа	1.0
Це стосується тих, хто працює від нашого імені	*Співробітники, консультанти, волонтери*
Підготовлено	Благодійний фонд «Благодійна організація «Стабілізейшен Суппорт Сервісез»»
Затверджено	Дермот Гамільтон
Дата затвердження	2020
Дата перезатвердження	Протягом двох років від дати затвердження

БЛАГОДІЙНА ОРГАНІЗАЦІЯ «БЛАГОДІЙНИЙ ФОНД «СТАБІЛІЗЕЙШЕН СУППОРТ СЕРВІСЕЗ»
CHARITABLE ORGANIZATION «CHARITY FOUNDATION «STABILIZATION SUPPORT SERVICES»
04053, Україна, м. Київ, вул. Січових Стрільців, 1-5
ЄДРПОУ 40567253, р/р 26008500242960 банк ПАТ «Креді Агріколь Банк», МФО 3006141

Політика інформаційної безпеки

1. Вступ

Комп'ютерна безпека при роботі в мережі є головною умовою успішної та продуктивної діяльності, оскільки дотримання основних її правил дозволяють захистити користувача від можливих ризиків втрати або псування важливої інформації, неправомірного використання його персональних даних, фінансових втрат і т.д.

1.1.Цілі

1.1.1. У Благодійній організації "Благодійний фонд "Стабілізейшен Суппорт Сервісез" в Україні (БО БФ "ССС") використовується локальна комп'ютерна мережа (ЛКМ), що дозволяє її користувачам отримати доступ до внутрішніх мережевих ресурсів (система управління ресурсами організації, прикладні задачі, електронна пошта, файли, принтери та ін.). Також ЛКМ підключена до інтернет. В ЛКМ працює велика кількість користувачів і їх робота повинна бути скоординована певними правилами для забезпечення стійкої роботи ЛКМ. Невиконання цих правил може призвести до збоїв в роботі ЛКМ і в результаті до збоїв в роботі всієї організації.

1.1.2. Метою цих Правил “Безпечної роботи в комп’ютерній мережі та за комп’ютером є:

- Опис коректної та безпечної роботи користувачів за комп'ютером, ЛКМ та інтернет.
- Забезпечення стійкої роботи ЛКМ та доступу в інтернет.

1.2. Сфера дії.

Комп’ютери і ЛКМ організації.

1.3. Визначення та абревіатури.

Організація

Благодійна організація "Благодійний фонд "Стабілізейшен Суппорт Сервісез", (БО "БФ "ССС").

БО "БФ "ССС"

Благодійна організація "Благодійний фонд "Стабілізейшен Суппорт Сервісез".

ЛКМ

Локальна комп'ютерна мережа.

ПЗ

Програмне забезпечення.

ІТ

Інформаційні технології

Системне програмне забезпечення

Забезпечує функціонування обладнання та зв'язок між обладнанням та стандартним та прикладним ПО. До нього відносяться BIOS, операційні системи, драйвери пристроїв і т.п.

Стандартне програмне забезпечення

Забезпечує безпеку роботи комп'ютера та роботу з документами. До нього відносяться
антивіруси, архіватори, програми Microsoft Office Word, Excel, PowerPoint, Outlook та ін.

Ресурси IT

Сукупність обладнання комп'ютер, ЛКМ, а також системного, стандартного та прикладного ПЗ.

Користувач

Користувач комп'ютером, ЛКМ або інтернет.

Робочі години

Час з 10:00 до 18:00 в робочі, вихідні та святкові дні.

2. Опис.

2.1. Створення нового користувача.

2.1.1. Отримати електронною поштою інформацію про нового співробітника, учасника програми та проекту від співробітника відділу Кадрів, а саме:
- Прізвище ім'я та по батькові;
- Назва особистої електронної пошти;
- Доступи до груп організації.

2.1.2. Створення облікового запису, додання його до робочих груп і надсилання листа з інструкцією для входження в обліковий запис користувачеві.

2.1.3. Купити і/або підготувати запитане обладнання (комп'ютер, принтер і т.п.) для нового співробітника, учасника програми та проекту.

2.1.4. Ознайомити нового співробітника, учасника програми та проекту з цими правилами, перевірити, що новий співробітник, учасник програми та проекту їх розуміє і дати йому необхідну інформацію про інфраструктуру IT.

2.1.5. Видати новому співробітнику, учаснику програми та проекту запитане обладнання.

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

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

2.2. Видалення користувача.

2.2.1. Отримати електронною поштою інформацію про звільнення співробітника, учасника програми та проекту від співробітника відділу Кадрів.

2.2.2. Блокування облікового запису.

2.2.3. Повернути все обладнання IT спеціалісту.

2.2.4. Перевірити все обладнання і його комплектність.

2.3. Використання обладнання.

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

2.4. Доступ до ресурсів IT.

Доступ до ресурсів IT суворо регламентований та захищений відповідними ідентифікаторами та паролями, які знає тільки Користувач. Час доступу до ресурсів IT не

обмежений, за випадком проведення встановлювальних, ремонтних або профілактичних робіт.

2.5. Підключення зовнішніх пристроїв для зберігання даних. Дозволяється підключати до службових комп'ютерів тільки перевірені антивірусом зовнішні пристрої для зберігання даних (USB флеш-пам'ять, картки пам'яті SD, MMS і інші, зовнішні жорсткі диски і т.і.).

2.6. Безпека комп'ютера, ПЗ і ЛКМ.

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

2.6.1. 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.

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

2.6.3. Залишати включений комп'ютер після роботи — будь ласка вимикайте комп'ютер після закінчення робочого часу.

2.6.4. Дозволяти стороннім людям використовувати ресурси ІТ.

2.6.5. Використовувати комп'ютер без антивірусу.

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

2.6.7. Встановлювати як на локальні, так і на мережеві диски любе програмне забезпечення (в т.ч. ігри). Виявлені неавторизоване програми будуть негайно та без попередження видалені.

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

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

2.6.10. Заходити на підозрілі і не захищені сайти в яких немає протоколу HTTPS, переходити по рекламним посиланням.

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

2.6.12. Користуватись не захищеними месенджерами.

У разі встановлення систематичного порушення цих правил співробітники ІТ мають право відключати користувачів від ресурсів ІТ.

Правила створення паролю.

2.7.1. Пароль повинен містити мінімум 8 символів.

2.7.2. 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 0 1 2 … 9
- Символи ` ~ ! @ # $ % ^ & * ( ) _ + - = { } | [ ] \ : " ; ' < > ? , . /

2.7.3. Пароль від облікового запису обов'язково потрібно закріплювати за телефонним номером, для подвійної аутентифікації.

2.7. Підключення до мережі Wi-Fi.

Для користування доступно три мережі:

- SSS
- SSS_5G
- SSS_Guest

Мережі SSS та SSS_5G використовуються лише працівниками організації через них є доступ до ЛКМ і пристроїв.

Мережа SSS_Guest використовується для доступу в інтернет гостям організації.

Забороняється розповсюджувати пароль мереж SSS та SSS_5G серед гостей організації.

2.8. Доступ до інтернет ресурсів організації.

Доступ до інтернет ресурсів організації надається з погодження керівника написанням електронного листа до IT-спеціаліста.

2.9. Бекап інформації

Необхідно щотижня робити резервне копіювання інформації на зовнішні пристрої і зберігати їх окремо від комп'ютера.

Директор
БО "БФ "Стабілізейшен Суппорт Сервісез" Дермот Гамільтон

02/12/20