БЛАГОДІЙНА ОРГАНІЗАЦІЯ
«БЛАГОДІЙНИЙ ФОНД «ЗАПОРІЗЬКЕ СЕРЦЕ»
Україна, 69035, Запорізька обл., м. Запоріжжя,
б. Примаченко Марії, будинок 11, офіс 705
тел. +38096185455; email: ngozpheart@gmail.com
ЄДРПОУ 45648263

ПОЛІТИКА ЦИФРОВОЇ БЕЗПЕКИ БЛАГОДІЙНОЇ ОРГАНІЗАЦІЇ «БЛАГОДІЙНОГО ФОНДУ «ЗАПОРІЗЬКЕ СЕРЦЕ»

2024 рік

Цей документ визначає принципи та основні засади цифрової Безпеки Благодійної організації "Благодійного фонду "Запорізьке серце"

Політика цифрової безпеки — це набір вимог, правил, обмежень та рекомендацій, які регламентують порядок роботи персоналу організації з інформацією. Реалізація цієї політики кожним членом структури спрямована на досягнення та підтримку стану цифрової безпеки всієї організації. Цифрова політика формується Правлінням організації, реалізується працівниками.

Метою політики цифрової безпеки е впровадження та ефективне управління системою забезпечення безпеки, спрямованої на:

- захист інформаційних активів організації,
- забезпечення стабільної діяльності організації;
- мінімізації ризиків у роботі організації, пов'язаних з втратою інформації;
- створення позитивних для організації інформаційних відносин з партнерами, клієнтами (бенефіціарів) та всередині структури;
- захист персональних даних членів організації, постачальників, партнерів, бенефіціарів.

Основним завданням інформаційної безпеки с захист інформаційних активів від зовнішніх та внутрішніх навмисних та ненавмисних загроз.

Фізичні заходи захисту

- усі офісні комп'ютери залишаються замкненими в приміщенні офісу підсигналізацією;
- кожен працівник організації мас особистий комп'ютер, яким користується виключно сам за принципом цифрової та інформаційної гігієни;
- робочий комп'ютер захищений паролем;
- резервне копіювання інформації організації зберігається на зовнішньомудиску та у хмарному сервісі;
- доступ до дуже чутливої інформації в організації обмежений;
- всі акаунти співробітників мають бути захищеними складним паролем тамати двофакторну авторизацію.

Апаратні засоби захисту

- робочі комп'ютери раз на рік відправляються на фізичну чистку до сервісу;
- кожен працівник працює в онлайн сервісах, що мають функцію автоматичного зберігання інформації, а у випадку використання інших програм обов'язково робить резервне копіювання на зовнішній диск та до хмарного сервісу;

- працівники використовують виключно перевірені носії інформації.

Програмні заходи захисту

- системне оновлення програмного забезпечення;
- використання іноземного програмного забезпечення лише за умови, що силові відомства та спецслужби країни виробника не матимуть доступу до інформації користувачів (таким чином, наразі для користування в організації заборонене програмне забезпечення вироблене в РФ);
- створення та використання виключно безпечних паролів працівниками організації;
- використання працівниками захисту паролем або шляхом шифрування чутливої інформації на своїй робочій машині;
- використання лише перевіреного та захищеного каналу передачі чутливої інформації між працівниками.

Просування політики цифрової безпеки в організації

Не рідше ніж раз на рік кожен працівник організації відвідує тренінги з цифрової безпеки, аби актуалізувати свої знання в цій царині та оволодівати новими інструментами захисту. Не рідше ніж раз на рік організація проводить аналіз корпоративної культури цифрової безпеки, прогнозує можливі зміни, визначає типи захисту для всієї інформації, яка с в організації, тощо. Відповідно до результатів аналізу, уточнюється система цифрового захисту інформації.

Поведінка персоналу

Благодійна організація "Благодійний фонд "Запорізьке серце" очікує від своїх співробітників цифрової поведінки, що підтримує позитивний імідж організації. З числа працівників організації призначається відповідальний за контроль заходів інформаційного захисту організації та облік і визначення рівня чутливості інформації в організації. При прийомі на роботу до організації нових працівників одним з етапів відбору с перевірка обізнаності з основ цифрової безпеки. За порушення вимог політики цифрової безпеки організація може передбачити заходи адміністративної та матеріальної відповідальності для всіх працівників.

Керівник організації Антон ОРЛОВ