ЗАТВЕРДЖЕНО
Протокол засідання Правління
ГО «Паросток»
від 27.01 2023 р. № 1
Голова зборів
Саранча І. Г. / /

ГРОМАДСЬКА ОРГАНІЗАЦІЯ ВІННИЦЬКА МІСЬКА ОРГАНІЗАЦІЯ СОЦІАЛЬНОГО РОЗВИТКУ ТА СТАНОВЛЕННЯ ОКРЕМИХ МАЛОЗАХИЩЕНИХ КАТЕГОРІЙ МОЛОДІ «ПАРОСТОК»

ПОЛІТИКА

цифрової безпеки

Вінниця - 2023

Політика цифрової безпеки Громадської організації Вінницька міська організація соціального розвитку та становлення окремих малозахищених категорій молоді «Паросток», далі ВМОСРСОМКМ «Паросток» — це набір вимог, правил, обмежень та рекомендацій, які регламентують порядок роботи персоналу організації з інформацією. Реалізація цієї політики кожним членом/нею Організації спрямована на досягнення та підтримку стану цифрової безпеки всієї Організації. Цифрова політика формується Правлінням ВМОСРСОМКМ «Паросток», реалізується її працівниками/ми.

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

- захист інформаційних активів Організації,
- забезпечення стабільної діяльності ВМОСРСОМКМ «Паросток»;
- мінімізації ризиків у роботі Організації, пов'язаних з втратою інформації;
- створення позитивних для організації інформаційних відносин з партнерами, клієнтами та всередині ВМОСРСОМКМ «Паросток».

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

Фізичні заходи захисту

- усі офісні робочі машини залишаються замкненими в приміщенні офісу під охороною;
- кожен працівник/ця Організації має свою особисту робочу машину, якою користується виключно сам/а за принципом цифрової та інформаційної гігієни;
- робоча машина захищається паролем;
- резервне копіювання інформації Організації зберігається на зовнішньому диску та у хмарному сервісі;
- доступ до дуже чутливої інформації в Організації обмежений.

Апаратні засоби захисту

- робоча машина раз на рік відправляється на фізичну чистку до сервісу;
- кожен працівник/ця щотижня обов'язково проводить перевірку своєї робочої машини на наявність шкідливих програм ;
- кожен працівник/ця щотижня обов'язково робить резервне копіювання на зовнішній диск та до хмарного сервісу;
- працівники/ці використовують виключно перевірені носії інформації.

Програмні заходи захисту

- використання лише ліцензійного програмного забезпечення;
- системне оновлення програмного забезпечення;
- використання іноземного програмного забезпечення лише за умови, що силові відомства та спецслужби країни виробника не матимуть доступу до інформації

користувачів/ок (таким чином, наразі для користування в організації заборонене програмне забезпечення вироблене в РФ)**;**

- створення та використання виключно безпечних паролів працівниками/ми Організації;
- використання працівниками/ми захисту паролем або шляхом шифрування чутливої інформації на своїй робочій машині;
- використання лише перевіреного та захищеного каналу передачі чутливої інформації між працівниками/ми.

Проєктування політики цифрової безпеки у ВМОСРСОМКМ «Паросток»

Не рідше ніж раз на рік кожен/а працівник/ця Організації відвідує тренінги з цифрової безпеки, аби актуалізовує 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 є в Організації, тощо. Відповідно до результатів аналізу, уточнюється система цифрового захисту інформації.

Поведінка персоналу

ВМОСРСОМКМ «Паросток» очікує від своїх співробітників/иць цифрової поведінки, що підтримує гарний імідж Організації. З числа працівників/иць ВМОСРСОМКМ «Паросток» призначається відповідальний/а за контроль заходів інформаційного захисту Організації та облік і визначення рівня чутливості інформації в Організації. При прийомі на роботу до ВМОСРСОМКМ «Паросток» нових працівників/иць одним з етапів відбору є перевірка обізнаності з основами цифрової безпеки. За порушення вимог політики цифрової безпеки Організація може передбачити заходи адміністративної та матеріальної відповідальності для всіх працівників/иць.