Administratorem w podmiocie o nazwie Zespół Szkół Chemiczno-Elektronicznych im. Jana Pawła II w Inowrocławiu jest dyrektor szkoły, tel. 52 353 72 10, adres ul. Poznańska 345, 88-100 Inowrocław, IOD: E. Harenda kontakt: zsche_iod@zsche.edu.pl

Zasady zabezpieczania systemów IT przed złośliwym oprogramowaniem w Zespole Szkół Chemiczno-Elektronicznych im. Jana Pawła II w Inowrocławiu

1. Systemy informatyczne należy chronić przed szkodliwym oprogramowaniem (np. wirusy, trojany, bomby logiczne, robaki) poprzez stosowanie odpowiednich środków technicznych i organizacyjnych.

2. Zidentyfikowanymi obszarami systemów informatycznych Administratora Danych Osobowych narażonymi na ingerencję wirusów oraz innego szkodliwego oprogramowania są dyski twarde lub karty pamięci urządzeń, elektroniczne nośniki informacji, dostęp do sieci publicznej, poczta e-mail.

3. Drogą przedostania się wirusów lub szkodliwego oprogramowania może być sieć publiczna, sieć lokalna lub elektroniczne nośniki informacji.

4. Stacje robocze, komputery przenośne, serwery muszą być objęte ochroną w czasie rzeczywistym za pomocą oprogramowania antywirusowego oraz zapory (firewall), zapewniających integralność zasobów przechowywanych i przetwarzanych w systemie informatycznym Administratora Danych Osobowych.

5. Oprogramowanie antywirusowe uruchamiane jest przy starcie systemu, a użytkownik nie posiada uprawnień do jego wyłączenia. Możliwość zatrzymania usługi systemu antywirusowego posiada jedynie Administrator Danych Osobowych lub Administrator szkolnej sieci komputerowej.

6. Konfiguracja programu antywirusowego zapewnia ciągłe monitorowanie otrzymywanych i wysyłanych, a także uruchamianych plików pod kątem występowania oprogramowania złośliwego.

7. System antywirusowy musi posiadać możliwość automatycznego skanowania każdego zewnętrznego elektronicznego nośnika informacji, który jest podłączany do urządzenia komputerowego.

8. W przypadku stwierdzenia pojawienia się wirusa i braku możliwości usunięcia go przez program antywirusowy, użytkownik powinien skontaktować się z Administratorem szkolnej sieci komputerowej.

9. W przypadku wystąpienia infekcji i braku możliwości automatycznego usunięcia wirusów przez system antywirusowy, Administrator szkolnej sieci komputerowej podejmuje działania zmierzające do usunięcia zagrożenia. W szczególności działania te mogą obejmować:

a) usunięcie zainfekowanych plików, o ile jest to akceptowalne ze względu na prawidłowe funkcjonowanie systemu informatycznego;

b) odtworzenie plików z kopii zapasowych, po uprzednim sprawdzeniu, czy dane zapisane na kopiach zapasowych nie są zainfekowane;

c) samodzielną ingerencję w zawartość pliku – w zależności od posiadanych kwalifikacji lub skonsultowanie się z odpowiednim serwisem.