Procedura zabezpieczania przed szkodliwym oprogramowaniem wykorzystywanym do prowadzenia nauki/pracy zdalnej w Szkole Podstawowej im. ks. Jana Twardowskiego w Powidzku

§ 1 Cel i zakres stosowania procedury

1. Celem procedury jest określenie zasad zapewniających zapobieganie, wykrywanie obecności i usuwanie szkodliwego oprogramowania.
2. Procedura przeznaczona jest dla wszystkich użytkowników systemów informatycznych.
3. Procedura ma charakter ogólny i ma zastosowanie do wszystkich systemów informatycznych wykorzystywanych w szkole.

§ 2 Oprogramowanie antywirusowe

1. Systemy informatyczne służące do przetwarzania informacji zabezpiecza się przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu poprzez stosowanie ochrony antywirusowej i systematyczne instalowanie aktualizacji systemów operacyjnych.
2. We wszystkich jednostkach organizacyjnych (sekretariat, kadry i księgowość, dyrektor, pedagog/psycholog) oraz w na komputerach w poszczególnych salach dydaktycznych i w pokojach nauczycielskich funkcjonuje oprogramowanie antywirusowe, którego wdrożenie, utrzymanie i zarządzanie jest koordynowane przez wychowawców i pracowników na samodzielnych stanowiskach.
3. Źródłami szkodliwego oprogramowania mogą być w szczególności wiadomości otrzymane pocztą elektroniczną wraz z załącznikami, strony internetowe, zewnętrzne nośniki informacji.
4. Oprogramowanie antywirusowe jest zainstalowane na: stacjach roboczych, urządzeniach mobilnych, laptopach.

§ 3 Obowiązki wychowawców klas i pracowników na samodzielnych stanowiskach

1. Oprogramowanie antywirusowe podlega systematycznej i automatycznej aktualizacji.
2. Należy również na bieżąco instalować poprawki bezpieczeństwa do systemów operacyjnych i użytkowych.
3. W/we osoby sprawują nadzór nad aktualizacjami, monitorują prawidłowość i skuteczność ich wykonania.

§ 4 Obowiązki użytkowników systemów

1. Zainstalowane i na bieżąco aktualizowane oprogramowanie antywirusowe ogranicza lecz nie eliminuje w pełni zagrożeń związanych z przedostaniem się do zasobów informatycznych złośliwego oprogramowania.
2. Zabronione jest wyłączanie ochrony antywirusowej.
3. Po podłączeniu nośnika zewnętrznego należy przeskanować go oprogramowaniem antywirusowym, przy czym zakazuje się podłączania nośników nieznanego pochodzenia.
4. Należy zwracać uwagę na nietypowe zachowania systemu informatycznego, takie jak:
   a) nieznane nowe pliki lub katalogi;
   b) nagłe zmniejszenie się ilości wolnego miejsca na dysku;
   c) nagły spadek wydajności stacji roboczej;
   d) nieoczekiwane efekty dźwiękowe, komunikaty a w szczególności z żądaniem okupu lub fikcyjnym zgłoszeniem do organów ścigania, itp.

   Wszystkie takie sytuacje należy zgłaszać dyrektorowi szkoły.

5. W przypadku stwierdzenia nietypowego zachowania komputera, które może być spowodowane działaniem złośliwego oprogramowania, a które nie zostało automatycznie wykryte i usunięte przy pomocy zainstalowanego oprogramowania antywirusowego, należy natychmiast przerwać pracę, i powiadomić dyrektora szkoły.
6. W przypadku braku dostępu do plików/katalogów lub komunikatów świadczących o zaszyfrowaniu danych (żądanie okupu, fikcyjne zgłoszenie do organów ścigania, itp.), zaleca się natychmiastowe wyłączenie komputera poprzez odłączenie zasilania w listwie zasilającej/ups lub wyciągnięcie wtyczki z gniazdka elektrycznego.

Powidzko, 25.03.2020 r.

Zaopiniował: Administrator danych:

....

(Inspektor Ochrony Danych Osobowych) (Dyrektor szkoły)