1. **Cel**

Określenie zasad dotyczących zabezpieczenia systemu informatycznego przed działalnością nieuprawnionego oprogramowania.

1. **Zakres obowiązywania**

Procedura obowiązuje wszystkich użytkowników upoważnionych do przetwarzania danych w systemie informatycznym oraz Administratora Systemów Informatycznych.

1. **Opis postępowania**
	1. Administrator Systemów Informatycznych jest zobowiązany do wprowadzenia obligatoryjnej ochrony antywirusowej, a także zabezpieczenia zaporą sieciową, która obejmuje wszystkie stacje robocze oraz serwery.
	2. Oprogramowanie antywirusowe powinno być skonfigurowane w sposób wymuszający automatyczne usuwanie oprogramowania złośliwego, zaś w przypadku gdy ich usunięcie jest niemożliwe, obejmowanie ich kwarantanną, okresowe skanowanie wszystkich dysków lokalnych, a także sporządzanie raportów oraz powiadamianie osoby odpowiedzialnej o wykrytym złośliwym oprogramowaniu.
	3. Dokonywanie zmian w konfiguracji oprogramowania antywirusowego oraz zapory sieciowej jest możliwa tylko przez Administratora Systemów Informatycznych.
	4. Przeprowadzane są okresowe szkolenia z zakresu bezpiecznej pracy z aplikacjami wykorzystywanymi na stacjach roboczych ze szczególnym uwzględnieniem aplikacji wykorzystywanych do łączności z systemami zewnętrznymi. Szkolenia powinny uświadamiać użytkownikom skalę i typy zagrożeń oraz metody jak ich uniknąć lub obniżyć prawdopodobieństwo cyberzagrożenia.
	5. Użytkownicy mający uprawnienia do korzystania z nośników zewnętrznych obowiązani są do sprawdzania programem antywirusowym wszelkich elektronicznych zewnętrznych nośników informacji.