ZAŁĄCZNIK NR 5 – INFORMACJA O SZCZEGÓLNYCH ZAGROŻENIACH ZWIĄZANYCH Z KORZYSTANIEM PRZEZ UŻYTKOWNIKÓW Z USŁUG ŚWIADCZONYCH DROGĄ ELEKTRONICZNĄ PRZEZ CENTRUM NAUCZANIA DOMOWEGO

Usługodawca wykonując obowiązek z art. 6 pkt 1) ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. 2020.344 t.j.), informuje o szczególnych zagrożeniach związanych z korzystaniem przez Klientów z usług świadczonych drogą elektroniczną. Informacja niniejsza dotyczy zagrożeń, które mogą wystąpić jedynie potencjalne, ale które powinny być brane pod uwagę, mimo zastosowania przez Usługodawcę środków zabezpieczających przed nieuprawnionym działaniem osób trzecich.

Do podstawowych zagrożeń związanych z korzystaniem z Platformy Edukacyjnej za pośrednictwem sieci Internetu należą:
− złośliwe oprogramowanie;
– różnego rodzaju aplikacje lub skrypty mające szkodliwe, przestępcze lub złośliwe działanie w stosunku do systemu teleinformatycznego wykorzystywanego przez Użytkownika, takie jak wirusy, robaki, trojany (konie trojańskie), keyloggery, dialery;
− programy szpiegujące (ang. spyware);
– programy śledzące działania Użytkownika, które gromadzą informacje o Użytkowniku i wysyłają je bez jego wiedzy i zgody Użytkownika - autorowi programu;
− spam, tj, niechciane i niezamawiane wiadomości elektroniczne rozsyłane jednocześnie do wielu odbiorców, często zawierające treści o charakterze reklamowym;
− wyłudzanie poufnych informacji osobistych (np. haseł) przez podszywanie się pod godną zaufania osobę lub instytucję (ang. phishing);
− włamania do systemu teleinformatycznego Użytkownika z użyciem m.in. takich narzędzi hackerskich jak exploit i rootkit.

Klient, w celu zminimalizowania ryzyka wystąpienia powyższych zagrożeń, powinien zainstalować oraz stale aktualizować program antywirusowy na swoim komputerze lub innym urządzeniu elektronicznym wykorzystywanym podczas pracy na Platformie Edukacyjnej.

Ochronę przed zagrożeniami związanymi z korzystaniem przez Użytkowników z usług świadczonych drogą elektroniczną zapewniają także:

− włączona zapora sieciowa (ang. firewall),
− aktualizacja wszelkiego oprogramowania wykorzystywanego do funkcjonowania systemu operacyjnego komputera lub innego urządzenia elektronicznego, które wykorzystuje Użytkownik,
− nieotwieranie załączników przesłanych Użytkownikowi pocztą elektroniczną od nieznanych adresatów,
− zapoznawanie się z treścią informacji zamieszczonych w okienkach instalacyjnych aplikacji, a także ich licencji,
− nieudostępnianie nieznanym osobom haseł lub innych danych dostępowych do Platformy Edukacyjnej oraz poczty elektronicznej Użytkownika
− regularne całościowe skany systemu operacyjnego programem antywirusowym,

- korzystanie z usługi sieci VPN,
- używanie oryginalnego systemu operacyjnego i aplikacji, pochodzących z legalnego źródła.