Załącznik nr 1

Informacja o szczególnych zagrożeniach związanych z korzystaniem przez użytkowników z usług świadczonych drogą elektroniczną.

1. REMONDIS Medison Sp. z o.o. wykonując obowiązek wynikający z treści art. 6 pkt 1 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (t.j. Dz. U. 2020 poz. 344), informuje o szczególnych zagrożeniach związanych z korzystaniem przez Usługobiorcę z Usług.
2. Informacja niniejsza dotyczy zagrożeń, które mogą wystąpić jedynie potencjalne, ale które powinny być brane pod uwagę, mimo stosowania środków zabezpieczających infrastrukturę przed nieuprawnionym działaniem osób trzecich.
3. Do podstawowych zagrożeń związanych z korzystaniem z sieci Internet należą:
    a) złośliwe oprogramowanie (ang. malware) – różnego rodzaju aplikacje lub skrypty mające szkodliwe, przestępcze lub złośliwe działanie w stosunku do systemu teleinformatycznego użytkownika sieci,
    b) programy szpiegujące (ang. spyware) – programy śledzące działania użytkownika, które gromadzą informacje o użytkowniku,
    c) spam - niechciane i niezamawiane wiadomości elektroniczne rozsyłane jednocześnie do wielu odbiorców, często zawierające treści o charakterze reklamowym,
    d) wyłudzanie poufnych informacji osobistych (np. haseł) przez podszywanie się pod godną zaufania osobę lub instytucję (ang. phishing),
    e) włamania do systemu teleinformatycznego użytkownika z użyciem m.in. takich narzędzi hackerskich jak exploit i rootkit.
4. Klient, aby uniknąć powyższych zagrożeń, powinien zaopatrzyć swój komputer i inne urządzenia elektroniczne, które wykorzystuje podłączając się do Internetu, w program antywirusowy. Program taki winien być stale aktualizowany.
5. Ochronę przed zagrożeniami związanymi z korzystaniem przez Klienta z usług zapewniają także:
    a. włączona zapora sieciowa (ang. firewall),
    b. aktualizacja oprogramowania,
    c. nieotwieranie załączników poczty elektronicznej niewiadomego pochodzenia,
    d. stosowanie programów antywirusowych i antymalware,
    e. szyfrowanie transmisji danych,
    f. instalacja programów prewencyjnych (wykrywania i zapobiegania włamaniom),
    g. używanie oryginalnego systemu i aplikacji, pochodzących z legalnego źródła.