Załącznik nr 2 do Regulaminu świadczenia usług drogą elektroniczną zasad korzystania przez Faktorantów z Serwisu internetowego znajdującego się pod adresem https://app.kalypso.pl/brewe

Na podstawie § 2 ust. 5 Regulaminu, zgodnie z art. 6 pkt 1 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz.U. z 2002 r. nr 144, poz. 1204 z późn. zm.) Usługodawca informuje o szczególnych zagrożeniach związanych z korzystaniem przez użytkowników z usług świadczonych drogą elektroniczną, które to zagrożenia stanowią potencjalne zagrożenia, które mogą wystąpić, a są to w szczególności:

- spam – niechciane i niezamawiane wiadomości elektroniczne rozsyłane jednocześnie do wielu odbiorów, często zawierające treści o charakterze reklamowym;
- wyłudzanie poufnych informacji osobistych (np. haseł) przez podszywanie się pod godną zaufania osobę lub instytucję (ang. Phishing);
- złośliwe oprogramowanie (ang. Malware) – różnego rodzaju aplikacje lub skrypty mające szkodliwe, przestępcze lub złośliwe działanie w stosunku do systemu teleinformatycznego użytkownika sieci, takie jak wirusy, robaki, trojany;
- programy szpiegujące (ang. Spyware) – programy śledzące działania użytkownika, które gromadzą informacje o użytkowniku i wysyłają je – zazwyczaj bez jego wiedzy i zgody – autorowi programu;
- włamania do systemu teleinformatycznego użytkownika z użyciem narzędzi hackerskich;
- kryptoanaliza – możliwość odnalezienia słabości systemu kryptograficznego w celu umożliwienia jego złamania lub obejścia.

Sugerowanym jest, aby Użytkownik pamiętał :

- należy regularnie uaktualniać system i oprogramowanie, które jest przez nas używane
- warto zaopatrzyć swój komputer w program antywirusowy, który ostrzeże nas przed niebezpieczeństwem
- nie należy otwierać hiperłączy bezpośrednio z otrzymanego e-maila, szczególnie jeśli nie znamy nadawcy wiadomości
- nie wolno przesyłać mailem żadnych danych osobistych - w żadnym wypadku nie wypełniajmy danymi osobistymi formularzy zawartych w wiadomości e-mail
- banki i instytucje finansowe stosują protokół HTTPS tam, gdzie konieczne jest zalogowanie do systemu. adres strony WWW rozpoczyna się wtedy od wyrażenia 'https://', a nie 'http://'. (jeśli strona z logowaniem nie zawiera w adresie nazwy protokołu HTTPS, powinno się zgłosić to naszym pracownikom i nie podawać na niej żadnych danych)
- każde podejrzenia co do sfingowanych witryn należy jak najszybciej przekazać policjantom lub naszym pracownikom odpowiedzialnym za jego funkcjonowanie w sieci.

Z uwagi na powszechny dostęp do komputera i urządzeń mobilnych uważajmy na to, komu pozwalamy korzystać z naszych kont i sprzętów. Nigdy nie należy podawać swoich danych do logowania osobom trzecim. Jeśli pozwalamy innym użytkownikom na podłączenie się do naszej sieci, ograniczajmy możliwość podłączania zewnętrznych nośników. Starajmy się regularnie wykonywać kopie bezpieczeństwa, a ważne dla nas pliki zapisywać na zewnętrznych nośnikach, odkładanych w niezagrożone miejsce. Stosując kilka prostych zasad możemy uniknąć stania się ofiarą internetowego przestępcy.