Podstawowe zasady dotyczące zapewnienia cyberbezpieczeństwa systemów informacyjnych w PWIK Sp. z o.o. w Koninie, opracowane dla Klientów/Kontrahentów Spółki

A. Najważniejsze definicje dotyczące zapewnienia cyberbezpieczeństwa w Przedsiębiorstwie Wodociągów i Kanalizacji Sp. z o.o. w Koninie, dalej jako „Spółka", o których mowa w ustawie z dnia 05.07.2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2018 r. poz. 1560):

1) ***cyberbezpieczeństwo*** - odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy;
2) ***incydent*** - zdarzenie, które ma lub może mieć niekorzystny wpływ na cyberbezpieczeństwo;
3) ***incydent krytyczny*** - incydent skutkujący znaczną szkodą dla bezpieczeństwa lub porządku publicznego, interesów międzynarodowych, interesów gospodarczych, działania instytucji publicznych, praw i wolności obywatelskich lub życia i zdrowia ludzi, klasyfikowany przez właściwy CSIRT MON, CSIRT NASK lub CSIRT GOV;
4) ***incydent poważny*** - incydent, który powoduje lub może spowodować poważne obniżenie jakości lub przerwanie ciągłości świadczenia usługi kluczowej;
5) ***incydent istotny*** - incydent, który ma istotny wpływ na świadczenie usługi cyfrowej w rozumieniu art. 4 rozporządzenia wykonawczego Komisji (UE) 2018/151 z dnia 30 stycznia 2018 r. ustanawiającego zasady stosowania dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 w odniesieniu do dalszego doprecyzowania elementów, jakie mają być uwzględnione przez dostawców usług cyfrowych w zakresie zarządzania istniejącymi ryzykami dla bezpieczeństwa sieci i systemów informatycznych, oraz parametrów służących do określenia, czy incydent ma istotny wpływ (Dz.Urz. UE L 26 z 31.01.2018, str. 48), zwanego dalej „rozporządzeniem wykonawczym 2018/151";
6) ***incydent w podmiocie publicznym*** - incydent, który powoduje lub może spowodować obniżenie jakości lub przerwanie realizacji zadania publicznego realizowanego przez podmiot publiczny, o którym mowa w art. 4 pkt 7-15;
7) ***zagrożenie cyberbezpieczeństwa*** - potencjalna przyczyna wystąpienia incydentu;
8) ***CSIRT NASK*** - Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym, prowadzony przez Naukową i Akademicką Sieć Komputerową – Państwowy Instytut Badawczy z siedzibą w Warszawie (01 – 045) przy ul. Kolskiej 12, tel.: 22 380 82 00 tel.: 22 380 82 01; e-mail: nask@nask.pl

B. Każdy incydent dotyczący naruszenia cyberbezpieczeństwa jest szczegółowo analizowany przez osoby powołane w Spółce do utrzymywania kontaktów z podmiotem krajowego systemu cyberbezpieczeństwa tj. z CSIRT NASK. Jeżeli incydent wyczerpuje znamiona „incydentu w podmiocie publicznym" Spółka jest zobowiązana to zgłosić do CSIRT NASK.

C. W Spółce zostały również opracowane dla Użytkowników – osób, na rzecz których zadanie publiczne jest realizowane, „Podstawowe zalecenia dotyczących cyberbezpieczeństwa systemów informacyjnych w PWIK Konin":

1) W czasie składania zleceń należy unikać korzystania z nieznanych urządzeń (publiczne komputery udostępniane w hotelach, bibliotekach, etc.).
2) W systemach operacyjnych, które tego wymagają, niezbędna jest instalacja i regularna aktualizacja oprogramowania antywirusowego.
3) Należy zachować ostrożność podczas pobierania plików z sieci Internet lub otwierania załączników należy zawsze przeczytać uważnie pojawiające się w przeglądarce komunikaty o alertach bezpieczeństwa i nigdy nie ignorować pojawiających się ostrzeżeń dotyczących zagrożeń ceberbezpieczeństwa.
4) W czasie składania zleceń transakcji należy unikać połączeń za pośrednictwem niezweryfikowanych sieci (publiczne WiFi).
5) Nie wolno instalować nieznanego oprogramowania otrzymanego pocztą elektroniczną lub pozyskanych z nieznanych lub niezaufanych źródeł.
6) Nigdy nie należy podłączać do komputera nieznanych nośników danych.
7) Nie wolno zezwalać osobom trzecim na manipulowanie urządzeniem mobilnym lub instalację oprogramowania.
8) Należy korzystać wyłącznie z legalnego oprogramowania pochodzącego ze znanego i zaufanego źródła.
9) Należy regularnie aktualizować posiadany system operacyjny oraz używane aplikacje, szczególności należy aktualizować przeglądarki internetowe, wtyczki flash, klientów poczty, przeglądarki plików pdf.
10) Nie wolno wyłączać mechanizmów bezpieczeństwa.
11) W zakresie logowanie się do systemów teleinformatycznych PWIK Konin zaleca się stosować poniższe zasady dotyczące siły hasła (hasło musi składać się minimum z 8 znaków oraz musi spełniać warunek złożoności polegający na występowaniu w nim: wielkiej i małej litery, cyfry lub znaku specjalnego, niedopuszczalne jest używanie tego samego hasła do różnych systemów oraz jego zapisywanie, hasło powinno być regularnie – co 30 dni zmieniane oraz nie może być nikomu udostępniane).