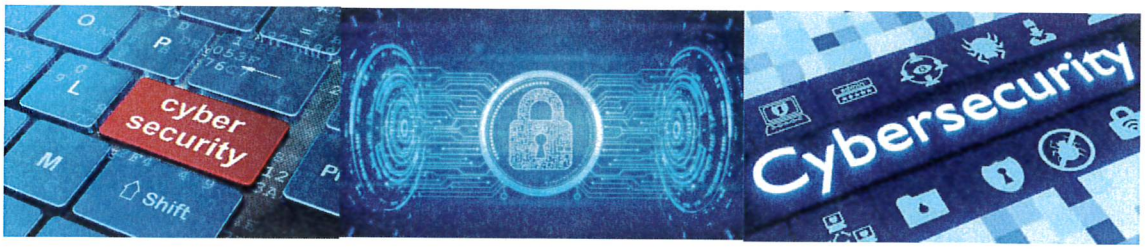

Podstawowe zasady dotyczące zapewnienia cyberbezpieczeństwa systemów informacyjnych w Przedsiębiorstwie Wodociągów i Kanalizacji Sp. z o.o. z siedzibą w Koninie, opracowane dla klientów (PZC)

1. Słownik pojęć:

Na potrzeby niniejszego dokumenty przyjmuje się następujące definicje:

1) **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, telefon ogólny: 22 380 82 00; e-mail ogólny: nask@nask.pl,
2) **cyberbezpieczeństwo** – odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy,
3) **iBOK** – internetowe Biuro Obsługi Klienta PWIK Konin,
4) **incydent** – zdarzenie, które ma lub może mieć niekorzystny wpływ na działalność PWIK Konin,
5) **incydent w podmiocie publicznym (ICPP)** – incydent, który powoduje lub może spowodować obniżenie jakości lub przerwanie realizacji zadania publicznego,
6) **interesariusz zewnętrzny** – osoba lub podmiot, który funkcjonuje poza strukturami organizacyjnymi PWIK Konin, klient, kontrahent,
7) **internet** – publiczna sieć telekomunikacyjna, niebędąca siecią wewnętrzną wykorzystywana głównie do świadczenia publicznie dostępnych usług telekomunikacyjnych w rozumieniu ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (Dz. U. z 2021 r. poz. 576 z późn. zm.),
8) **klient** – interesariusz zewnętrzny, który jest stroną zawartej z PWIK Konin umowy na dostawę wody i/lub odprowadzanie ścieków,
9) **PWIK Konin (Spółka)** – Przedsiębiorstwo Wodociągów i Kanalizacji Sp. z o.o. z siedzibą w Koninie,
10) **system informacyjny** – System teleinformatyczny wraz z przetwarzanymi w nim danymi w postaci elektronicznej,
11) **system teleinformatyczny** – zespół współpracujących ze sobą urządzeń i oprogramowania zapewniający przetwarzanie, przechowywanie, a także wysyłanie i odbieranie danych przez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci urządzenia końcowego,
12) **uksc** – ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2020 r. poz. 1369 z późn. zm.)
13) **urządzenie końcowe** – urządzenie telekomunikacyjne podłączone bezpośrednio lub pośrednio do zakończenia sieci (w szczególności: stacja robocza, terminal lub inne urządzenie pozwalające użytkownikowi na dostęp do systemu informacyjnego),
14) **urządzenie telekomunikacyjne** – urządzenie przeznaczone do zapewnienia nadawania, odbioru lub transmisji informacji, niezależnie od ich rodzaju, za pomocą przewodów, fal radiowych bądź optycznych lub innych środków wykorzystujących energię elektromagnetyczną,
15) **użytkownik** – klient zarejestrowany w iBOK,
16) **zadanie publiczne** – realizowane przez PWIK Konin jako podmiot publiczny w rozumieniu uksc zadania publiczne dotyczące ujmowania, uzdatniania lub dostarczania wody, odprowadzania lub oczyszczanie ścieków.

2. Podstawowe zasady dotyczące cyberbezpieczeństwa

Każdy incydent dotyczący naruszenia cyberbezpieczeństwa jest szczegółowo analizowany przez odpowiednio wyznaczone i wykwalifikowane do tego osoby spośród struktur wewnętrznych powołanych w Spółce. Osoby te uprawnione są do utrzymywania kontaktów z CSIRT NASK.
Jeżeli incydent wyczerpuje znamiona incydentu w podmiocie publicznym Spółka jest zobowiązana to zgłosić do CSIRT NASK.

2.1. PWIK Konin opracował dla interesariuszy zewnętrznych, w szczególności klientów oraz kontrahentów podstawowe zasady dotyczące cyberbezpieczeństwa systemów informacyjnych w PWIK Konin, zgodnie z którymi:
   1) należy unikać korzystania z nieznanych urządzeń (publicznych komputerów udostępnianych 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 internetu lub otwierania załączników,
   4) należy zapoznać się z pojawiającymi się w przeglądarce komunikatami o alertach bezpieczeństwa, jednocześnie nie ignorując pojawiających się ostrzeżeń dotyczących zagrożeń cyberbezpieczeństwa,
   5) należy unikać połączeń za pośrednictwem niezweryfikowanych sieci (publiczny dostęp do internetu),
   6) nie należy instalować nieznanego oprogramowania otrzymanego pocztą elektroniczną lub pozyskanego z nieznanych lub niezaufanych źródeł,
   7) nie należy podłączać do komputera nieznanych nośników danych,
   8) nie należy zezwalać osobom trzecim na modyfikację urządzeń lub instalację oprogramowania,
   9) należy korzystać wyłącznie z legalnego oprogramowania pochodzącego ze znanego i zaufanego źródła,
   10) należy regularnie aktualizować posiadany system operacyjny oraz używane aplikacje (w szczególności przeglądarki internetowe, wtyczki flash, klientów poczty),
   11) nie należy wyłączać mechanizmów bezpieczeństwa,
   12) logując się do systemów teleinformatycznych PWIK Konin zaleca się stosowanie poniższych zasad dotyczących siły hasła:
      a) hasło powinno składać się z minimum z 8 znaków oraz powinno spełniać warunek złożoności polegający na występowaniu w nim wielkiej i małej litery, cyfry lub znaku specjalnego,
      b) nie zaleca się używania tego samego hasła do różnych systemów oraz jego zapisywania.
      c) hasło powinno być regularnie – co 30 dni – zmieniane oraz nie może być nikomu udostępniane.

2.2. W celu zapewnienia bezpieczeństwa systemów teleinformatycznych, PWIK Konin podejmuje działania własne związane z rozszerzeniem poziomu bezpieczeństwa poprzez:
   1) potwierdzanie tożsamości klientów przy korzystaniu z iBOK,
   2) procesy autoryzacji związane z podmiotem, który może zatwierdzić treść, wydać lub podpisać kluczowe dokumenty transakcji,
   3) zapewnienie, że klienci są w pełni poinformowani o ich autoryzacji do korzystania z iBOK,
   4) określenie i spełnienie wymagań poufności, dostępności i integralności, przedstawienia dowodu wysyłki i odbioru dokumentów,
   5) utrzymanie poziomu zaufania wymaganego w stosunku do integralności kluczowych dokumentów,
   6) określenie wymagań dotyczących ochrony informacji poufnych,
   7) określenie wymagań dotyczących ochrony danych osobowych,
   8) zapewnienie poufności, dostępności, autentyczności i integralności wszystkich transakcji,
   9) unikanie strat lub powielania informacji o transakcjach,
   10) odpowiedzialność związaną z transakcjami oszukańczymi,
   11) wymagania dotyczące ubezpieczenia.

2.3. W związku z realizacją zadania publicznego PWIK Konin nie nadaje klientom dostępów w innych systemach niż iBOK. Wymiana danych pomiędzy PWIK Konin a klientami odbywa się przez iBOK oraz pocztę elektroniczną.