

Miejskie Przedsiębiorstwo Wodociągów i Kanalizacji w m.st. Warszawie S.A.	Wymagania w zakresie zachowania bezpieczeństwa informacji	Strona 1/6 Załącznik IN-ZSZ-01/04 Wydanie 02 z 21.01.2026 r.
---	--	--

1. Wymagania ogólne

- 1.1 Wykonawca, który świadczy usługi na rzecz i na terenie Spółki musi działać zgodnie z mającymi zastosowanie przepisami prawa oraz regulacjami wewnętrznymi Spółki w zakresie ochrony informacji, w tym ochrony danych osobowych.
- 1.2 Niniejsze wymagania obowiązują wszystkich wykonawców uzyskujących dostęp do informacji posiadanych przez Spółkę (np. przetwarzających, przechowujących, przesyłających dane lub dostarczających elementy infrastruktury teleinformatycznej dla przetwarzania informacji należących do Spółki).
- 1.3 Wykonawca jest zobowiązany do przeszkolenia pracowników i osób trzecich realizujących w jego imieniu zadania na rzecz przedmiotu Umowy w zakresie zachowania zasad bezpieczeństwa informacji, przedstawionych w niniejszym dokumencie.
- 1.4 Wykonawca jest zobowiązany do wykonania przedmiotu Umowy w sposób niepowodujący zaprzestania lub zakłócenia pracy infrastruktury teleinformatycznej Zamawiającego. Powyższe nie dotyczy elementów infrastruktury Zamawiającego, których wyłączenie z eksploatacji lub ograniczenie eksploatacji Strony uzgodniły.

2. Przetwarzanie informacji udostępnionych przez Spółkę

- 2.1 Wszystkie informacje przekazane Wykonawcy przez Spółkę (w formie papierowej, elektronicznej, ustnej itp.) podlegają ochronie. Wykonawca zobowiązany jest, w trakcie realizacji umowy/zlecenia, do stosowania następujących zasad:
 - 1) przy przetwarzaniu udostępnionych lub powierzonych informacji, należy szczególnie zadbać o zachowanie poufności, integralności i dostępności tych informacji;
 - 2) wykonawca bez zgody Spółki nie może udostępniać lub publikować informacji o realizowanej umowie lub informacji dotyczących Spółki powziętych podczas świadczenia umowy;
 - 3) informacje zapisane na nośnikach danych należy przekazywać z zastosowaniem protokołu zdawczo-odbiorczego;
 - 4) na etapie rozpoczęcia współpracy z podmiotem zewnętrznym (np. realizacja umowy) należy ustalić sposób szyfrowania informacji i plików elektronicznych, które mają być przesyłane przy wykorzystaniu poczty elektronicznej; tam, gdzie jest to technicznie możliwe, należy stosować zabezpieczenia kryptograficzne z algorytmem co najmniej 128 bit;
 - 5) zbędne wydruki, notatki, kserokopie dokumentów, mapy sieci, dokumenty projektowe itp. zawierające informacje należące do Spółki muszą być bezwzględnie niszczone w sposób uniemożliwiający odtworzenie ich treści. Za skuteczne zniszczenie tych dokumentów

Miejskie Przedsiębiorstwo Wodociągów i Kanalizacji w m.st. Warszawie S.A.	Wymagania w zakresie zachowania bezpieczeństwa informacji	Strona 2/6 Załącznik IN-ZSZ-01/04 Wydanie 02 z 21.01.2026 r.
---	--	--

odpowiedzialna jest osoba, która do momentu daty przydatności odpowiedzialna była za ich przechowywanie;

- 6) wydruki zawierające dane należące do Spółki po zakończeniu pracy muszą być przechowywane w zamkniętych szafach, bez dostępu do nich osób nieupoważnionych;
- 7) przestrzegać obowiązujących zasad postępowania z danymi osobowymi, które są określone w Rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).

2.2 Zabronione jest:

- 1) przekazywanie nośników informacji zawierających dane Spółki podwykonawcom współpracującym z wykonawcami bez umowy zachowania poufności, a w przypadku danych osobowych umowy powierzenia przetwarzania danych;
- 2) pozostawiania bez nadzoru lub udostępnianie osobom nieupoważnionym informacji (w formie elektronicznej, papierowej itp.) przekazanych przez Spółkę,
- 3) przekazywania informacji, należących do Spółki, pozyskanych lub zauważonych podczas realizacji zadań, osobom lub podmiotom nieuprawnionym do ich pozyskania.

3. Wykonawcy korzystający ze sprzętu komputerowego

3.1 Wykonawcy korzystający ze sprzętu komputerowego (komputery, urządzenia mobilne, telefony itp.) zobowiązani są do:

- 1) używania tylko legalnego oprogramowania;
- 2) używania oprogramowania antywirusowego z aktualną bazą wirusów;
- 3) stosowania silnych haseł;
- 4) natychmiastowej zmiany hasła, jeśli istnieje podejrzenie, że zostało ono ujawnione innej osobie niż Wykonawca;
- 5) ustawienia ekranów stanowisk z dostępem do danych udostępnianych przez Spółkę (w pomieszczeniach, gdzie przebywają osoby postronne) w taki sposób, żeby uniemożliwić tym osobom wgląd w dane;
- 6) zabezpieczenia dostępu do systemu informatycznego przed dostępem osób nieuprawnionych (zablokowanie ekranu lub wylogowanie się z systemu), w przypadkach chwilowego opuszczenia stanowiska pracy;
- 7) wykorzystywania urządzeń mobilnych do transmisji informacji, wyłącznie wtedy, gdy przekaz jest szyfrowany;
- 8) wykorzystywania sieciowych technologii bezprzewodowych do transmisji informacji, wyłącznie wtedy, gdy przekaz jest szyfrowany;
- 9) wylogowania się z systemu informatycznego natychmiast po zakończeniu pracy w tym

Miejskie Przedsiębiorstwo Wodociągów i Kanalizacji w m.st. Warszawie S.A.	Wymagania w zakresie zachowania bezpieczeństwa informacji	Strona 3/6 Załącznik IN-ZSZ-01/04 Wydanie 02 z 21.01.2026 r.
---	--	--

systemie.

3.2 Zabronione jest:

- 1) przesyłanie danych z systemu informatycznego osobom nieuprawnionym do odbioru takich danych;
- 2) logowanie się z wykorzystaniem identyfikatora i hasła osoby trzeciej;
- 3) udostępnianie identyfikatora i hasła osobom trzecim;
- 4) informowanie o infrastrukturze informatycznej Spółki, stosowanych zabezpieczeniach, wykorzystywanych systemach informatycznych osób trzecich, niezwiązanych z realizacją usługi;
- 5) stosowanie oprogramowania z naruszeniem warunków stosownej licencji;
- 6) testowanie lub podejmowanie prób poznania metod zabezpieczenia sieci i systemów informatycznych Spółki;
- 7) podejmowanie prób obejścia zabezpieczeń systemów informatycznych.

4. Dostęp wykonawców do sieci i systemów informatycznych

- 4.1 Dostęp do infrastruktury teleinformatycznej Spółki jest przyznawany w celu i w zakresie realizacji postanowień umowy zawartej pomiędzy wykonawcą i Spółką.
- 4.2 Dostęp jest udzielany po podpisaniu umowy wraz z oświadczeniem o zachowaniu poufności oraz po zapoznaniu się z zasadami bezpieczeństwa informacji obowiązującymi w Spółce oraz podpisaniu zobowiązania do zachowania poufności przetwarzanych danych.
- 4.3 W przypadku danych osobowych dostęp jest udzielany po podpisaniu umowy wraz z oświadczeniem o zachowaniu poufności, podpisaniu umowy powierzenia danych osobowych oraz po zapoznaniu się z zasadami bezpieczeństwa informacji obowiązującymi w Spółce.
- 4.4 Podłączany sprzęt musi mieć zainstalowane aktualne oprogramowanie antywirusowe oraz dostęp do zasobów ograniczony do niezbędnego minimum.
- 4.5 Dostęp do infrastruktury teleinformatycznej Spółki możliwy jest wyłącznie poprzez VPN.
- 4.6 Dostęp udzielany jest dla maksymalnie czterech pracowników wykonawcy. W uzasadnionych przypadkach, na pisemny wniosek wykonawcy zatwierdzony przez upoważnioną w Spółce osobę, liczba udzielonych dostępów może być wyższa.
- 4.7 Korzystanie z systemów informatycznych Spółki jest możliwe na następujących zasadach:
 - 1) wykonawca jest jednoznacznie zidentyfikowany przez system teleinformatyczny jako użytkownik posiadający swój unikalny, nadany przez pracownika Spółki identyfikator (login);
 - 2) hasła kont uprzywilejowanych składają się z minimum piętnastu znaków zawierających małe litery, duże litery, cyfry oraz znaki specjalne. Hasła dostępowe muszą być zmieniane okresowo, maksymalnie co trzydzieści dni;

Miejskie Przedsiębiorstwo Wodociągów i Kanalizacji w m.st. Warszawie S.A.	Wymagania w zakresie zachowania bezpieczeństwa informacji	Strona 4/6 Załącznik IN-ZSZ-01/04 Wydanie 02 z 21.01.2026 r.
---	--	--

- 3) dostęp VPN do infrastruktury Spółki jest zabezpieczony poprzez dwuskładnikowe uwierzytelnienie, wykorzystujące jednorazowy token dostępu przesyłany poprzez dedykowaną aplikację telefonii komórkowej;
- 4) zdalna obsługa może być prowadzona jedynie z wykorzystaniem urządzeń, które posiadają aktualne zabezpieczenia antywirusowe oraz zainstalowane niezbędne łatki/ aktualizacje bezpieczeństwa;
- 5) wykonawca musi za każdym razem zgłaszać zamiar logowania lub wylogowania do zasobów IT/OT mailowo na adres poczty elektronicznej:
zgloszenia.serwisu@mpwik.com.pl:
 - a) zgłoszenie musi mieć temat: „Zgłoszenie zamiaru logowania do infrastruktury – nazwa firmy – nawiązanie połączenia” lub „Zgłoszenie zamiaru logowanie do infrastruktury – nazwa firmy – zakończenie połączenia”;
 - b) w zgłoszeniu należy podać:
 - imię i nazwisko serwisanta,
 - czas zalogowania lub wylogowania,
 - zaplanowany zakres prac do wykonania,
 - nazwę zasobu (systemu) na którym będą wykonywane prace;
- 6) połączenia zdalne i prace wykonywane przez pracowników Wykonawcy za pomocą tego połączenia są monitorowane i nagrywane;
- 7) w przypadku zakończenia świadczenia usługi Wykonawca zobowiązany jest bezzwłocznie zaprzestać korzystania z posiadanych dostępów.

4.8 Zabronione jest:

- 1) niezgodne z ustalonymi procedurami, nienadzorowane próby łączenia z bezprzewodową siecią korporacyjną, o ile nie jest to bezwzględnie wymagane do realizacji umowy;
- 2) samodzielne wpinanie urządzeń do sieci informatycznej;
- 3) dla urządzeń komputerowych pracujących w sieci LAN zestawianie innych połączeń niż połączenia autoryzowane przez Spółki;
- 4) testowanie lub podejmowania prób poznania metod zabezpieczenia sieci i systemów informatycznych Spółki;
- 5) obchodzenie zabezpieczeń systemów informatycznych;
- 6) skanowanie sieci teleinformatycznej Spółki.

Miejskie Przedsiębiorstwo Wodociągów i Kanalizacji w m.st. Warszawie S.A.	Wymagania w zakresie zachowania bezpieczeństwa informacji	Strona 5/6 Załącznik IN-ZSZ-01/04 Wydanie 02 z 21.01.2026 r.
---	--	--

5. Wprowadzanie zmian i modyfikacje w infrastrukturze teleinformatycznej

- 5.1 Zmiany w infrastrukturze teleinformatycznej Zamawiającego, z wyjątkiem nowych projektów, muszą być prowadzone zgodnie z wewnętrznymi procedurami Spółki.
- 5.2 Modyfikacje lub zmiany zaplanowane do wprowadzenia w infrastrukturze teleinformatycznej powinny, tam gdzie jest to możliwe, być wykonane najpierw w środowisku testowym, a następnie po zatwierdzeniu modyfikacji lub zmiany w środowisku produkcyjnym.
- 5.3 W każdym przypadku wprowadzania zmian w infrastrukturze teleinformatycznej, osoba wykonująca czynności serwisowe jest zobligowana do wykonania archiwizacji konfiguracji zasobu przed rozpoczęciem prac w celu umożliwienia odtworzenia modyfikowanej konfiguracji przez innego administratora/pracownika strony trzeciej.
- 5.4 Przed wprowadzeniem modyfikacji lub zmiany Wykonawca musi przeprowadzić analizę ryzyka związanego z wprowadzeniem modyfikacji lub zmiany.

6. Incydynty

- 6.1 W przypadku stwierdzenia naruszenia lub zaistnienia okoliczności wskazujących na naruszenie bezpieczeństwa informacji Wykonawca jest zobowiązany bezzwłocznie powiadomić osobę odpowiedzialną za prawidłową realizację umowy o zaistniałej sytuacji. Wskazana osoba postępuje dalej zgodnie z wewnętrznymi procedurami Spółki.
- 6.2 Jeżeli wykonawca zauważy:
 - 1) obce osoby bez identyfikatora, poruszające się bez opieki;
 - 2) pozostawione dokumenty przekazane przez Spółkę;
 - 3) korzystanie z obcego identyfikatora lub hasła;
 - 4) niezamknięte, pozostawione bez opieki pomieszczenia;
 - 5) niezablokowany komputer lub urządzenie mobilne z dostępem do systemów informatycznych;
 - 6) wykorzystywanie zdalnego połączenia VPN przez osoby nieupoważnione;
 - 7) pozostawioną bez nadzoru dokumentację;
 - 8) inne zdarzenia, które wg własnej oceny stanowią zagrożenie dla bezpieczeństwa informacji
 - bezzwłocznie zgłasza je do osób pod opieką których przebywa w trakcie realizacji zadań dla Spółki.
- 6.3 Jeżeli Wykonawca zauważy wszelkie nieprawidłowości i podejrzaną aktywność zasobów IT/OT bezzwłocznie zgłasza ten fakt za pomocą poczty elektronicznej na adres: incydenty@mpwik.com.pl lub telefonicznie pod nr 22 445 73 33.

Miejskie Przedsiębiorstwo Wodociągów i Kanalizacji w m.st. Warszawie S.A.	Wymagania w zakresie zachowania bezpieczeństwa informacji	Strona 6/6 Załącznik IN-ZSZ-01/04 Wydanie 02 z 21.01.2026 r.
---	--	--

6.4 Incydenty wynikające z działań pracownika wykonawcy związane z:

- 1) nieuprawnionym dostępem do systemu informatycznego Spółki;
- 2) łamaniem haseł;
- 3) deszyfracją plików;
- 4) nieautoryzowanymi próbami łamania zabezpieczeń;
- 5) próbą wejścia do pomieszczeń niezwiązanych z realizowaną usługą;
- 6) udostępniania przepustki i hasła osobie trzeciej;
- 7) nieuprawnione udostępnianie danych osobowych będą uważane za ciężkie naruszenie obowiązującej umowy ze Spółką.