Załącznik nr 1
do umowy powierzenia
przetwarzania informacji/
danych osobowych
nr .....
z dnia .....

Podstawowe zasady bezpieczeństwa informacji/ochrony danych osobowych (PZBI) w stosunku do dostawców/wykonawców i ich pracowników świadczących dostawy/usługi na rzecz Przedsiębiorstwa Wodociągów i Kanalizacji Sp. z o.o. w Koninie, opracowane na podstawie rozporządzenia MSWiA z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. Nr 100, poz. 1024)

1. Obszar przetwarzania informacji chronionych/danych osobowych u Dostawcy/Wykonawcy jest zabezpieczony przed dostępem osób nieuprawnionych na czas nieobecności w nim osób upoważnionych do przetwarzania danych osobowych poprzez system kontroli dostępu do pomieszczeń biurowych.
2. Pomieszczenia biurowe Dostawcy/Wykonawcy są zamykane na klucz. Każdy pracownik Dostawcy/Wykonawcy odpowiada za swój klucz. W przypadku zagubienia klucza należy niezwłocznie poinformować o tym fakcie swojego bezpośredniego przełożonego.
3. Przebywanie osób nieuprawnionych w obszarze przetwarzania informacji chronionych/danych osobowych jest dopuszczalne w siedzibie Przedsiębiorstwa Wodociągów i Kanalizacji Sp. z o.o. w Koninie, dalej jako „ADO" za jego zgodą lub w obecności osoby upoważnionej do przetwarzania informacji/danych osobowych.
4. W systemie informatycznym ADO, służącym do przetwarzania informacji chronionej/danych osobowych stosuje się mechanizmy kontroli dostępu do tych danych.
5. W celu ochrony usług sieciowych przed nieautoryzowanym dostępem upoważnieni pracownicy ADO sprawuje kontrolę nad wszystkimi urządzeniami i systemami podłączanymi do sieci.
6. Każde podłączane do sieci urządzenie lub system Dostawcy/Wykonawcy musi spełniać minimalne wymagania bezpieczeństwa określone przez Administratora Systemu Informatycznego, dalej jako „ASI" – pracownika ADO.
7. W celu ochrony poufności informacji przetwarzanych w systemach informatycznych ADO, wszystkie osoby uzyskujące dostęp do ww. systemów muszą być zobowiązane w formie pisemnej do zachowania w tajemnicy informacji chronionych u ADO, zgodnie z wymaganiami Polityki Bezpieczeństwa Informacji (PBI) oraz Instrukcji Zarządzania Systemem Informatycznym (IZSI), obowiązującymi u ADO.
8. Pracownicy Dostawcy/Wykonawcy oraz inne osoby niebędące pracownikami ADO, starające się o dostęp do informacji chronionych/danych osobowych ADO utrzymują upoważnienia do przetwarzania danych osobowych wydane przez Administratora Bezpieczeństwa Informacji, dalej jako „ABI" – pracownika ADO oraz dodatkowo są zobowiązane do podpisania oświadczenia o zachowaniu w poufności danych osobowych/informacji oraz sposobów ich zabezpieczenia.

9. Jeżeli dostęp do informacji chronionej/danych osobowych przetwarzanych w systemie informatycznym posiadają co najmniej dwie osoby, wówczas ASI zapewnia, aby: w systemie tym rejestrowany był dla każdego użytkownika - Dostawcy/Wykonawcy odrębny identyfikator (login); dostęp do informacji chronionych/danych osobowych był możliwy wyłącznie po wprowadzeniu identyfikatora oraz hasła (dokonaniu uwierzytelnienia użytkownika).
10. Identyfikator użytkownika (login) - Dostawcy/Wykonawcy, który utracił uprawnienia do przetwarzania informacji chronionych/danych osobowych, nie może być przydzielony innej osobie.
11. Uwierzytelniania użytkownika - Dostawcy/Wykonawcy w systemie informatycznym ADO, przetwarzającym informacje chronione/dane osobowe odbywa się poprzez wpisania identyfikatora użytkownika (loginu) oraz hasła. Zmian hasła następuje nie rzadziej niż co 30 dni. Hasło składa się co najmniej z 8 znaków, zawiera małe i wielkie litery oraz cyfry lub znaki specjalne.
12. Informacje chronione/dane osobowe przetwarzane w systemie informatycznym Dostawcy/Wykonawcy są zabezpieczone poprzez wykonywanie kopii zapasowych zbiorów danych oraz programów służących do ich przetwarzania.
13. Kopie zapasowe, o których mowa w pkt. 12 niniejszych PZBI:
    a) są przechowywane w miejscach zabezpieczających je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem, każdorazowo wyznaczonym przez Dostawcę/Wykonawcę,
    b) usuwa się niezwłocznie po ustaniu ich użyteczności.
14. W sytuacji gdy użytkownik - pracownik Dostawcy/Wykonawcy przy realizacji niniejszej umowy korzysta z urządzeń mobilnych/elektronicznych nośników informacji jest zobowiązany zabezpieczyć te dane w sposób zapewniający poufność i integralność tych danych oraz zachować szczególną ostrożność podczas ich transportu, przechowywania i użytkowania poza obszarem przetwarzania informacji chronionej/danych osobowych, w tym jest zobowiązany stosować w ww. urządzeniach środki ochrony kryptograficznej (szyfrującej) wobec przetwarzanych informacji chronionych/danych osobowych.
15. Urządzenia, dyski lub inne elektroniczne nośniki informacji, będące własnością ADO, a przekazywane pracownikom Dostawcy/Wykonawcy, zawierające informacje chronione/dane osobowe, przeznaczone do:
    a) likwidacji - pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie;
    b) przekazania podmiotowi nieuprawnionemu do przetwarzania danych - pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie;
    c) naprawy - pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem osoby upoważnionej przez ADO.
16. Dostawca/Wykonawca jest zobowiązany do monitorowania wdrożonych zabezpieczeń systemu informatycznego.
17. ADO ma prawo w związku z zawartą umową do kontroli zabezpieczeń informatycznych (elektronicznych) oraz zabezpieczeń tradycyjnych Dostawcy/Wykonawcy.
18. System informatyczny służący do przetwarzania informacji chronionej/danych osobowych u Dostawcy/Wykonawcy powinien być chroniony przed zagrożeniami pochodzącymi z sieci publicznej poprzez wdrożenie fizycznych i logicznych zabezpieczeń chroniących przed nieuprawnionym dostępem do tych systemów.

19. W przypadku zastosowania logicznych zabezpieczeń, o których mowa w pkt. 17 niniejszych PZBI, obejmują one:
    a) kontrolę przepływu informacji pomiędzy systemem informatycznym Dostawcy/Wykonawcy a siecią publiczną;
    b) kontrolę działań inicjowanych z sieci publicznej i systemu informatycznego ADO.
20. System informatyczny Dostawcy/Wykonawcy służący do przetwarzania informacji chronionych/danych osobowych jest zabezpieczony, w szczególności przed:
    a) działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego poprzez stosowanie oprogramowania antywirusowego;
    b) utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej poprzez stosowanie UPS podtrzymującego pracę serwerowni.
21. Pracownicy Dostawcy/Wykonawcy są zobowiązani przy realizacji umowy do stosowania środków kryptograficznej (szyfrującej) ochrony wobec danych wykorzystywanych do uwierzytelnienia (loginów i haseł), które są przesyłane w sieci publicznej.
22. W celu ograniczenia ryzyka nieuprawnionego dostępu, utraty lub uszkodzenia informacji/danych osobowych w czasie godzin pracy i poza nimi pracownicy Dostawcy/Wykonawcy są zobowiązani:
    a) po zakończeniu pracy przechowywać dokumenty zawierające informacje chronione/dane osobowe i wymienne nośniki komputerowe w odpowiednio zabezpieczonych zamkami meblach biurowych,
    b) nie pozostawiać komputerów bez nadzoru w stanie aktywnej sesji dostępu do sieci,
    c) po zakończeniu pracy wylogować się z systemu i wyłączyć komputer, niedopuszczalne jest zakończenie pracy bez wykonania pełnej i poprawnej procedury zamknięcia lub przez wyłączenie napięcia zasilającego,
    d) po zakończeniu pracy do uporządkowania swojego stanowisko pracy, uniemożliwiając tym samym dostęp osób nieupoważnionych do informacji chronionych/danych osobowych,
    e) przestrzegać zasady niepozostawiania otwartych i niezabezpieczonych drzwi oraz okien podczas nieobecności w pomieszczeniu osób upoważnionych do przetwarzania informacji/danych osobowych,
    f) używać wygaszaczy ekranu zabezpieczonych hasłem,
    g) zabezpieczać nieużywany w danym momencie komputer przed nieupoważnionym dostępem, włączając blokadę systemową; ponowny dostęp do komputera następuje dopiero po podaniu hasła,
    h) ustawiać monitory komputerów w taki sposób, żeby uniemożliwić osobom nieupoważnionym wgląd w zawartość ekranu,
    i) odpowiednio zabezpieczyć miejsca przyjmowania/wysyłania korespondencji papierowej oraz odbioru/wysyłania faksów,
    j) włączać blokadę urządzeń kopiujących, zabezpieczając je w ten sposób przed nieuprawnionym użyciem osób nieupoważnionych,
    k) zwracać uwagę i przekazywać zauważone, pozostawione bez nadzoru oryginały lub kopie w pobliżu urządzeń kserograficznych swojemu bezpośredniemu przełożonemu,
    l) zwracać szczególną uwagą na pracujące drukarki pozostawione bez nadzoru,
    m) nie pozostawiać bez nadzoru wymiennych nośników komputerowych w napędach, bądź ogólnie dostępnych miejscach,
    n) niszczyć niepotrzebne dokumenty papierowe w niszczarkach, za wyjątkiem nośników zawierających informacje wrażliwe, których sposób niszczenia regulują odrębne przepisy.

Załącznik nr 2
do umowy powierzenia
przetwarzania informacji/
danych osobowych
nr .....
z dnia .....

Oświadczenie Dostawcy/Wykonawcy

Oświadczam, że zostałem zapoznany z „Podstawowymi zasadami bezpieczeństwa informacji (PZBI)" obowiązującymi w Przedsiębiorstwie Wodociągów i Kanalizacji Sp. z o.o. w Koninie oraz zobowiązuję się do ich przestrzegania pod rygorem zapłaty kar umownych, o których mowa w umowie powierzenia przetwarzania informacji/danych osobowych nr ..... z dnia .....

.....
(data, czytelny podpis Dostawcy/Wykonawcy)