

### **Regulamin dostępu do sieci VPN Aquanet SA.**

Regulamin określa jednolite i wiążące zasady postępowania w przypadku dostępu do systemów Zamawiającego przez Wykonawcę, szczegółowy opis procesu zarządzania dostępem dla Wykonawcy do systemów informatycznych oraz ustanawia zasady pracy pod ścisłą kontrolą dysponenta informacji Zamawiającego

1. Terminy użyte w treści oznaczają:

**System** - System informatyczny Zamawiającego

**VPN** – połączenia sieciowe zrealizowane w architekturze „client-to-site”

**Wykonawca** - Podmiot zewnętrzny korzystający z prawa dostępu do Systemu zgodnie z zapisami umowy.

**Konto** – Poświadczenia tożsamości w systemie informatycznym dla osoby upoważnionej przez Wykonawcę do świadczenia usług zgodnie z zapisami umowy. Konto jest przypisane do osoby reprezentującej Wykonawcę w związku z tym Wykonawca może posiadać wiele kont dostępowych.

**AD (active directory)** – usługa katalogowa (LDAP) dla systemów Microsoft Windows 2008 i młodszych.

**System przesiadkowy** – komputer z systemem operacyjnym Microsoft Windows 2012 lub nowszy z autentykacją AD, osiągalny tylko przez prawidłowo działający VPN.

2. Zasady dostępu do systemu

- 2.1. Dostęp do Systemu Zamawiającego dla Wykonawcy możliwy jest wyłącznie dla uprawnionych przedstawicieli Wykonawcy, którzy otrzymali stosowną zgodę na prowadzenie prac i wypełnili obowiązek zgłoszenia konieczności przeprowadzenia prac w systemie Zamawiającego.
- 2.2. Przedstawicielem Wykonawcy może być osoba, która akceptuje postanowienia (umowy/porozumienia) i realizuje prace za wiedzą i pod nadzorem Zamawiającego.
- 2.3. Wszelkie działania Wykonawcy polegające na dostępie do systemów Zamawiającego poza nadzorowanymi sesjami, utrudniające działanie lub powodujące destabilizację systemu są niedopuszczalne.

- 2.4. Dostęp realizowany jest tylko i wyłącznie na wskazany przez Zamawiającego system informatyczny i przez formalnie przekazane przez Zamawiającego metody.
3. Wniosek o dostęp
  - 3.1. Wniosek o nadanie dostępu realizowany jest przez umocowanego do obsługi umowy pracownika Zamawiającego Wniosek należy przesłać formalnie w systemie obiegu dokumentów Zamawiającego (SZD „Wniosek o nadanie uprawnień”) i zawierać następujące informacje:
    - 3.1.1. Dane użytkownika wnioskującego o dostęp (nazwa konta AD)
    - 3.1.2. numer umowy dla której realizowany jest dostęp VPN
4. Autentykacja, autoryzacja, metody dostępu do systemu.
  - 4.1. Realizacja dostępu do systemu odbywa się na podstawie prawidłowej autentykacji w usłudze AD.
  - 4.2. Wniosek o utworzenie konta AD, wystawienie certyfikatu VPN oraz innych poświadczeń realizowany jest zgodnie z formalnym obiegiem dokumentów w spółce wspieranym dedykowanym formularzem systemu SZD,
  - 4.3. Dla bieżącej kontroli Zamawiający będzie nagrywał sesje dla każdego zestawionego połączenia VPN,
  - 4.4. Konta usługi AD są blokowane automatycznie w przypadku 30 dniowego braku aktywności na koncie,
  - 4.5. Konto usługi AD może być nadane na czas określony jednak nie dłuższy niż okres obowiązywania umowy z Wykonawcą,
  - 4.6. Konto usługi AD może być aktywowane tylko i wyłącznie na czas określony przez Zamawiającego jako niezbędny dla realizacji zapisów umowy np. dla obsługi konkretnego zdarzenia,
  - 4.7. certyfikat połączenia VPN zabezpieczony jest hasłem,
  - 4.8. certyfikat połączenia VPN jest wydawany na czas określony,
  - 4.9. Połączenie do systemu możliwe jest tylko i wyłącznie przez wskazany przez Zamawiającego ‘system przesiadkowy’,
  - 4.10. Praca z systemem jest możliwa w środowisku systemu przesiadkowego oraz w sesjach RDP, SSH itd. inicjowanych na systemie przesiadkowym.
5. Lista warunków dostępu
  - 5.1. Otrzymanie zgody na dostęp.
  - 5.2. Wniosek o dostęp
  - 5.3. Zgoda na dostęp zwyczajowo zapisana jest w Umowie pomiędzy stronami, której załącznikiem jest niniejszy regulamin.
6. Zobowiązania i odpowiedzialność Wykonawcy
  - 6.1. Zarejestrowani przedstawiciele Wykonawcy są wyłącznie osobami, których działania mają doprowadzić do dojścia do skutku czynności prawnych pomiędzy Zamawiającym, a wykonawcą (Stronami tych czynności), zgodnie z

wymaganiami umowy (umów) zawartych pomiędzy Zamawiającym, a Wykonawcą i ponoszą odpowiedzialność z tytułu istniejących, bądź mogących się ujawnić w przyszłości roszczeń Zamawiającego i Wykonawcy, a wynikających z nie dojdęcia do skutku zadań objętych przedmiotem umowy lub umów.

- 6.2. Wykonawca świadczy usługi wynikające z zawartych umów z zastrzeżeniem dopuszczalnych przerw technicznych, niezbędnych do prawidłowego funkcjonowania systemu, oraz zgodnie z ustanowionym niniejszym regulaminem dostępu chyba, że przerwa techniczna jest następstwem okoliczności, których Wykonawca nie był w stanie przewidzieć.
  - 6.3. Wykonawca ponosi odpowiedzialność za ujawnienie przez Wykonawcę osobom trzecim danych zawartych w Systemie.
  - 6.4. Zamawiający uprawniony jest do zablokowania dostępu Wykonawcy do systemu w przypadku, gdy czynności podejmowane przez Wykonawcę naruszają postanowienia regulaminu, zawartych umów lub obowiązujące przepisy prawa, bądź negatywnie wpływają na dobre imię Zamawiającego. Zablokowanie dostępu Dostawcy z powodów jak wyżej opisanych nie zwalnia go z obowiązków, do których dotrzymania zobowiązany jest wykonawca w ramach umowy.
  - 6.5. W przypadku, gdy działania Wykonawcy naruszają postanowienia regulaminu, negatywnie wpływają na dobre imię Zamawiającego, bądź innych użytkowników systemu Zamawiającego, bądź w inny sposób są szkodliwe, bądź niezgodne z prawem Zamawiający uprawniony jest wedle własnego wyboru do:
    - 6.5.1. zawieszenia na czas określony lub nieokreślony dostępu VPN dla Wykonawcy;
    - 6.5.2. ograniczenia na czas określony lub nieokreślony dostępu VPN do wszystkich, bądź poszczególnych usług świadczonych w ramach systemów Zamawiającego;
    - 6.5.3. podjęcia właściwych czynności prawnych.
  - 6.6. Niezależnie od zawieszenia dostępu VPN, Wykonawca ponosi pełną odpowiedzialność odszkodowawczą określoną w umowie za swoje działania i zaniechania, będące podstawą dokonanego zawieszenia dostępu VPN, w szczególności względem Zamawiającego.
  - 6.7. W okresie zawieszenia Wykonawca nie korzysta z żadnych innych usług świadczonych przez Zamawiającego w ramach systemów Zamawiającego.
7. Przykłady działań niepożądanych
- 7.1.1. Wykorzystywanie poświadczeń przypisane do innego użytkownika,
  - 7.1.2. Przeglądanie aplikacji/danych nie związanych z obsługą deklarowanego zgłoszenia,
  - 7.1.3. Próba modyfikacji logów systemowych,

- 7.1.4. Próba zakładania nowych lub modyfikacja istniejących kont użytkowników bez uzgodnienia z Zamawiającego
- 7.1.5. Próba kopiowania danych bez uzgodnienia z Zamawiającym,
- 7.1.6. Inne naruszające poufność, integralność i dostępność danych (informacji).

8. Wymagania techniczne dla realizacji umowy:

- 8.1 Zamawiający przygotowuje certyfikat i konfigurację dla realizacji połączenia VPN oraz udzieli podstawowych informacji o sposobie realizacji połączenie VPN. Konfiguracja urządzeń Wykonawcy jest po stronie Wykonawcy.
- 8.2 Zamawiający przygotowuje konta w usłudze AD dla systemu przesiadkowego, oraz poświadczenia dla kont systemów będących przedmiotem umowy.
- 8.3 Zamawiający decyduje o liczbie i nazewnictwie kont i poświadczeń dla systemów.