

Regulamin Zarządzania Bezpieczeństwem OT w Aquanet SA

Załącznik 2.

Regulamin udzielania dostępu dostawcom do zasobów

1. Wykonawca zobowiązuje się do stosowania ogólnie przyjętych zasad bezpieczeństwa informatycznego, w szczególności tych opisanych w niniejszym dokumencie.
2. Dostęp do jakichkolwiek systemów informatycznych, systemów automatyki, systemów energetyki Zamawiającego (dalej zwanych: „Zasobami”) przyznawany jest zgodnie z obowiązującą u Zamawiającego Polityką Bezpieczeństwa Zamawiającego oraz Regulaminem Zarządzania Bezpieczeństwem OT Zamawiającego (dalej zwanych łącznie: „Polityką Bezpieczeństwa”) za pośrednictwem opiekuna Umowy po stronie Zamawiającego, który ma prawo domagać się potwierdzenia przez Wykonawcę spełnienia warunków wynikających z Polityki Bezpieczeństwa.
3. Podstawową metodą dostępu do Zasobów Zamawiającego jest:
 - a) Przydzielenie imiennego dostępu zdalnego za pomocą VPN client to site do sieci IT Zamawiającego (dalej zwanej: „Siecią”),
 - b) Uzyskanie dostępu do stacji przesiadkowej pozwalającej na monitorowanie sesji użytkowników z dostępem do dalszych zasobów – zgodnie z przydzielonymi uprawnieniami,
 - c) Do dyspozycji Wykonawcy zgodnie z przydzielonymi uprawnieniami oprócz stacji przesiadkowej będą inne Zasoby w zależności od potrzeb wynikających z realizacji Umowy.
4. Zamawiający może narzucić wykonywanie prac wyłącznie na własnych stacjach inżynierskich.
5. Zamawiający dopuszcza wykorzystywanie urządzeń Wykonawcy (dalej zwane: „Urządzeniem”), z możliwością podłączenia do Sieci, pod warunkiem spełnienia poniższych zasad:
 - a) Odebrania od Wykonawcy oświadczenia iż:
 - Urządzenie jest wolne od oprogramowania szkodliwego, szpiegującego i elementów, które mogą negatywnie wpłynąć na inne urządzenia działające w Sieci,
 - Na Urządzeniu jest zainstalowana aplikacja zabezpieczająca posiadająca co najmniej funkcjonalność ochrony antywirusowej z ochroną w czasie rzeczywistym,
 - Zainstalowane na Urządzeniu oprogramowanie spełnia kryteria oprogramowania legalnego,
 - Urządzenie nie będzie realizowało skanów i monitorowania Sieci, chyba że jest to niezbędne do wykonania Umowy.
 - b) Weryfikacji przez administratora właściwego dla Zasobu (dalej zwany: „Administratorem”) dla którego wykonywane są prace przez Wykonawcę:
 - zainstalowania na Urządzeniach systemu antywirusowego wraz z najnowszymi aktualizacjami,
 - zainstalowania na Urządzeniach poprawek krytycznych systemu operacyjnego.
 - c) Uzgodnienia z Zamawiającym konfiguracji sieci urządzenia (TCP/IP, nazwa netbios).
6. Decyzję o podłączeniu Urządzeń podejmuje Administrator dla którego wykonywane są prace przez Wykonawcę.
7. Podłączenie będzie możliwe zgodnie z decyzją Administratora do dedykowanego segmentu Sieci (DMZ) w celu ochrony Zasobów za pomocą minimalnych reguł firewall lub w wyjątkowych przypadkach bezpośrednio do Sieci.

8. Zamawiający dopełni wszelkich starań, żeby zapewnić odpowiedni poziom bezpieczeństwa dla urządzeń działających w infrastrukturze Zamawiającego, jednocześnie nie odpowiada za jakiegokolwiek szkody wynikające z użytkowania w ten sposób Urządzenia Wykonawcy.
9. Zabronione jest podłączanie do Sieci urządzeń sieciowych (router, accesspoint, repeater wifi, itp.) mających na celu wygenerowanie ruchu sieciowego poza bezpośredni obszar Sieci. Podłączenie takich urządzeń zostanie potraktowane jako świadome działanie godzące w bezpieczeństwo teleinformatyczne Zamawiającego. Zapis ten nie dotyczy sytuacji, w której Zamawiający zleca Wykonawcy instalację takiego urządzenia.
10. Wykonawca świadomy jest, że Sieć jest monitorowana, w związku z czym zgadza się na kontrolę ruchu wygenerowanego przez jego Urządzenia wpięte do Sieci, bezpośrednio lub za pośrednictwem dostępu zdalnego. Monitorowanie nie obejmuje skanowania zawartości i ingerencji w Urządzenie oraz nie obejmuje wglądu w treść korespondencji.
11. Zamawiający zastrzega sobie prawo do odłączenia danego Urządzenia od Sieci bez uprzedniego powiadomienia w przypadku, gdy zaistnienie podejrzenia, że takie urządzenie stanowi jakiegokolwiek zagrożenie dla infrastruktury Zamawiającego. Blokada następuje do czasu wyjaśnienia powyższego zagrożenia. Działanie takie nie powoduje przedłużenia terminów realizacji przedmiotu Umowy.
12. Zamawiający zastrzega sobie prawo do całkowitego odebrania uprawnień pracownikowi Wykonawcy lub jego podwykonawcy oraz wstępu na obiekt, któremu wykazano świadome rażące łamanie zapisów niniejszego dokumentu. Działanie takie nie powoduje przedłużenia terminów realizacji przedmiotu Umowy.
13. Wykonawca odpowiada za dotrzymanie warunków dopuszczenia sprzętu do pracy w Sieci i może zostać poproszony o udowodnienie ich spełnienia.
14. Wykonawca odpowiada za świadome lub nieświadome działania związane z naruszeniem zasad bezpieczeństwa Zamawiającego spowodowane złym stanem Urządzenia Wykonawcy podłączonym do Sieci lub oprogramowaniem na nim zainstalowanym, w tym także oprogramowaniem szkodliwym.
15. Zamawiający może dochodzić od Wykonawcy, w przypadku powstania szkody, związanej z niewykonywaniem postanowień niniejszego dokumentu, odszkodowania na zasadach ogólnych.
16. W przypadku zaistnienia sytuacji naruszenia bezpieczeństwa teleinformatycznego, za które odpowiedzialny jest Wykonawca lub osoba przez niego zatrudniona lub z nim współpracująca, Wykonawca jest zobowiązany do zwrotu Zamawiającemu wszelkich kosztów związanych z usunięciem powstałej szkody.
17. Wykonawca jest zobowiązany ustalić z Administratorem, na którym wykonuje prace sposób bezpiecznego przekazywania kodów źródłowych, haseł oraz innych danych dostępowych i technicznych.
18. Wykonawca przygotowujący oprogramowanie dla sterowników PLC i HMI może korzystać wyłącznie z następujących platform:
 - a) TIA v17
 - b) Step7 Professional 2021/v5.7
 - c) WinCC Flexible 2008 SP3
 - d) LOGOSoft! V8.2
 - e) EcoStruxure Control Expert v15
 - f) VijeoDesigner v6.2 SP11
 - g) EcoStruxure Machine Expert – Basic 1.2
19. Wykonawca przygotowujący dokumentację do systemów OT może korzystać wyłącznie z następujących programów:

- a) SEE Electrical V8R4 – część rysunkowa (opcja preferowana)
- b) Inne programy CAD z możliwością eksportu do formatu DWG - część rysunkowa (opcja dopuszczalna)
- c) MS Office – część opisowa