

Wymagania Bezpieczeństwa dla Systemów DCS/SCADA w Grupie QEMETICA

07.02.2024

Spis Treści

1.0	Wykaz skrótów i definicji	3
2.0	Wymagania dotyczące segmentacji sieci	5
3.0	Polityka haseł	6
4.0	Wymagania dotyczące uwierzytelniania	7
5.0	Zarządzanie dostępem do Zasobów Przemysłowych	8
6.0	Redundancja Systemów i Infrastruktury IT Przemysłowego	10
7.0	Bezpieczeństwo Systemów IT Przemysłowego	10
8.0	Bezpieczeństwo Stacji Inżynierskich	11
9.0	Bezpieczeństwo Stacji Operatorskich	12
10.0	Zdalny dostęp	12

1.0 Wykaz skrótów i definicji

AKPIA – aparatura kontrolno-pomiarowa i automatyka

Business Unit – podmioty biznesowe wchodzące w skład Grupy QEMETICA zgodnie z obowiązującą strukturą organizacyjną

Cienki Klient - komputer bądź specjalizowane urządzenie (terminal komputerowy) wraz z odpowiednim oprogramowaniem typu klient, umożliwiające obsługę aplikacji stworzonej w architekturze klient-serwer.

Infrastruktura IT Przemysłowego – Serwery Przemysłowe, Stacje Operatorskie, Stacje Inżynierskie, urządzenia sieciowe

Incydent Bezpieczeństwa – każde zdarzenie związane z nieprzestrzeganiem zasad uwzględnionych w niniejszej Polityce lub każde zdarzenie mające wpływ na dostępność, poufność i integralność Zasobów IT Przemysłowego

Instalacje Przemysłowe – Skomplikowana i rozbudowana infrastruktura, znajdująca się wewnątrz bądź na zewnątrz budynku lub innego obiektu przemysłowego. Przeznaczona jest do obiegu mediów na terenie obiektu umożliwia prowadzenie procesów produkcyjnych.

Konto techniczne (Runtime) – konto wykorzystywane podczas instalacji komponentów systemów przemysłowych, konto niezbędne do prawidłowej pracy operacyjnej Systemu Przemysłowego i wykonywania działań utrzymaniowych, rozwojowych i serwisowych na podsystemie

Konto techniczne – konto z uprawnieniami uprzywilejowanymi, wykorzystywane do uwierzytelniania na poziomie system – system lub usługa-usługa.

Konto serwisowe – lokalne konto z uprawnieniami uprzywilejowanymi, wykorzystywane przez dostawców i dział IT Przemysłowego do logowania się na poziomie systemu operacyjnego w celu wykonania prac utrzymaniowych, rozwojowych i serwisowych

Konto administracyjne – domenowe konto z uprawnieniami uprzywilejowanymi wykorzystywane do działań rozwojowych na zasobach zarejestrowanych w usłudze katalogowej (Active Directory)

Konto współdzielone – lokalne konto wykorzystywane do uwierzytelniania do Systemów Przemysłowych z poziomu Cienkiego Klienta do Stacji Operatorskich i Stacji Inżynierskich

PAM – Privileged Access Management

Systemy Przemysłowe / Systemy IT Przemysłowego – systemy wspierające proces sterownia i nadzoru nad procesami technologicznymi, systemy raportujące pracę AKPiA.

Serwery Przemysłowe – fizyczne lub zwirtualizowane serwery, na których zostały zainstalowane Systemy Przemysłowe.

Stacje Operatorskie - Stacje służące do sterowania pracą instalacji przez obsługę, zazwyczaj system posiada kilka takich singlowych lub redundantnych stacji, często wielomonitorowych.

Stacje Inżynierskie – Stacje przeznaczone do programowania i wprowadzania zmian w programie sterownia. Stacja nie jest wymagana dla ciągłej pracy instalacji, dzięki niej można jednocześnie wprowadzać zmiany i obserwować zmiany.

Środowiska wyspowe – Serwery Przemysłowe, Stacje Operatorskie, Stacje Inżynierskie, Systemy Przemysłowe nie podłączone do sieci IT Przemysłowego i odseparowane na poziomie sieci.

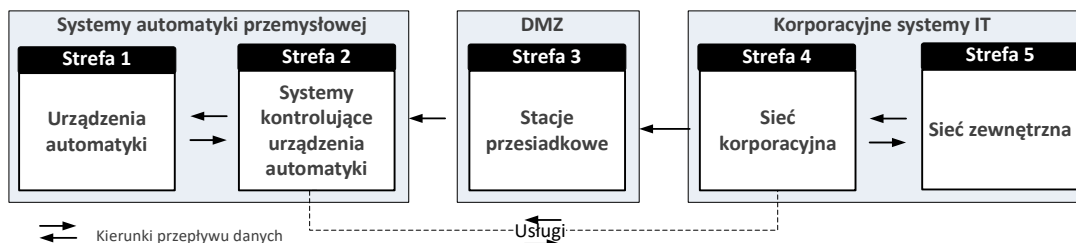
Zarząd – Zarząd QEMETICA S.A.

Zasoby IT Przemysłowego / IT Przemysłowe – Systemy Przemysłowe oraz Infrastruktura IT Przemysłowego

Zespół IT Przemysłowego – wydzielona w strukturach organizacyjnych jednostka, odpowiedzialna za utrzymanie, zarządzanie i rozwój Zasobów IT Przemysłowego z uwzględnieniem ustalonego podziału ról i odpowiedzialności

2.0 Wymagania dotyczące segmentacji sieci

- W celu zapewnienia bezpieczeństwa Zasobów IT Przemysłowego, zasada segmentacji sieci zakłada, iż dozwolony jest bezpośredni przepływ danych tylko pomiędzy sąsiadującymi strefami z uwzględnieniem dopuszczalnych wyjątków w komunikacji na poziomie usług pomiędzy Strefą 2 a Strefą 4.



Rys. Model segmentacji sieci

- Poniżej znajdują się zasady komunikacji sieciowej odzwierciedlone na grafice powyżej.
 - Zasady komunikacji sieciowej dla Strefy 1 – Urządzenie Automatyki
 - Niedopuszczalna jest komunikacja sieciowa do Strefy 1 ze Strefy 3,4,5
 - Dopuszczalna jest komunikacja dwukierunkowa do Strefy 1 tylko ze Strefy 2
 - Zasady komunikacji sieciowej dla Strefy 2 – Systemy kontrolujące urządzenia automatyki
 - Niedopuszczalna jest komunikacja do Strefy 2 ze Strefy 5
 - Niedopuszczalna jest komunikacja bezpośrednia na poziomie Użytkownika do Strefy 2 ze Strefy 4
 - Dopuszczalna jest komunikacja sieciowa dwukierunkowa na poziomie usług pomiędzy Strefą 2 i Strefą 4
 - Dopuszczalna jest komunikacja sieciowa jednokierunkowa dla zdalnych sesji Użytkowników zewnętrznych do Strefy 2 ze Strefy 4
 - Dopuszczalna jest komunikacja jednokierunkowa pomiędzy Strefą 3 i Strefą 1
 - Dopuszczalna jest komunikacją dwukierunkową pomiędzy Strefą 1 i Strefą 2
 - Dopuszczalna jest tymczasowa sieciowa komunikacja dwukierunkowa do strefy 3 ze strefy 2 na potrzeby zespołu IT Przemysłowego
 - Zasady komunikacji sieciowej dla Strefy 3 – Stacje przesiadkowe
 - Niedopuszczalna jest komunikacja sieciowa do Strefy 3 ze Strefy 5
 - Niedopuszczalna jest komunikacja sieciowa ze Strefy 3 do Strefy 1
 - Dopuszczalna jest komunikacja sieciowa jednokierunkowa na poziomie Użytkownika ze Strefy 3 do Strefy 2
 - Dopuszczalna jest komunikacja sieciowa jednokierunkowa na poziomie Użytkownika do Strefy 3 ze Strefy 4
 - Dopuszczalna jest tymczasowa sieciowa komunikacja dwukierunkowa do strefy 4 ze strefy 3 na potrzeby zespołu IT Przemysłowego

- Zasady komunikacji sieciowej dla Strefy 4 – Sieć korporacyjna
 - Niedopuszczalna jest komunikacja sieciowa ze Strefy 4 do Strefy 2 na poziomie Użytkownika
 - Niedopuszczalna jest komunikacja sieciowa ze Strefy 4 do Strefy 1
 - Dopuszczalna jest komunikacja sieciowa jednokierunkowa ze strefy 4 do strefy 3 na poziomie Użytkownika
 - Dopuszczalna jest komunikacja sieciowa dwukierunkowa pomiędzy Strefą 4 do Strefy 5
 - Dopuszczalna jest komunikacja sieciowa dwukierunkowa na poziomie usług pomiędzy Strefą 4 a Strefą 2
- Zasady komunikacji sieciowej dla Strefy 5 – Sieć zewnętrzna
 - Niedopuszczalna jest komunikacja sieciowa ze Strefy 5 do Stref 3,4,5 na poziomie
 - Dopuszczalna jest komunikacja sieciowa dwukierunkowa pomiędzy Strefą 5 i Strefą 4

3.0 Polityka haseł

- W celu zapewnienia odpowiedniego poziomu ochrony kont wykorzystywanych przez Zasoby IT Przemysłowego wymagana jest poniższa polityka haseł.
 - Konta użytkowników
 - Hasło musi zawierać **co najmniej** 10 znaków długości, w tym **co najmniej**:
 - jedną wielką literę (A-Z) oraz
 - jedną małą literę (a-z),oraz **co najmniej**:
 - jedną cyfrę (0-9) **oraz opcjonalnie jeden znak specjalny**.
 - W przypadku kont domenowych maksymalny okres ważności haseł wynosi 60 dni.
 - Konta administracyjne
 - Hasło musi zawierać **co najmniej** 12 znaków długości, w tym **co najmniej**:
 - jedną wielką literę (A-Z) oraz
 - jedną małą literę (a-z),oraz **co najmniej**:
 - jedną cyfrę (0-9) **oraz opcjonalnie jeden znak specjalny**.
 - W przypadku kont domenowych maksymalny okres ważności haseł wynosi 30 dni.
 - Konta Techniczne, Konta Techniczne (Runtime), Konta Serwisowe
 - Hasło musi zawierać **co najmniej** 12 znaków długości, w tym **co najmniej**:
 - jedną wielką literę (A-Z) oraz
 - jedną małą literę (a-z),oraz **co najmniej**:

- jedną cyfrę (0-9) **oraz opcjonalnie jeden znak specjalny**.
- W przypadku kont domenowych maksymalny okres ważności haseł wynosi: bezterminowo

4.0 Wymagania dotyczące uwierzytelniania

- Dostęp logiczny do Zasobów IT Przemysłowego wymaga uwierzytelnienia. Uwierzytelnianie, to proces potwierdzania deklarowanej tożsamości cyfrowej, w celu ochrony zasobów przed dostępem osób nieuprawnionych, dlatego każdy użytkownik powinien posiadać jednoznacznie przypisany identyfikator (login) wyłącznie do swojego osobistego użytku, wszędzie tam gdzie jest to technicznie i operacyjnie możliwe – wyjątek stanowią konta funkcyjne lub serwisowe.
- Dostawca DCS zapewni, że włączone lub utworzone zostaną wyłącznie konta niezbędne do obsługi systemu sterowania z hasłami zdefiniowanymi przez użytkownika, skonfigurowanymi podczas instalacji systemu.
- Wymagane jest rozwiązanie „password less” na potrzeby uwierzytelniania do stacji operatorskich znajdujących się w pomieszczeniach ze stałą obsługą, o ściśle ograniczonym, monitorowanym i kontrolowanym dostępie fizycznym, wszędzie tam gdzie jest wymagany ciągły dostęp do Systemów Przemysłowych.
- Uwierzytelnianie w Zasobach IT Przemysłowego musi następować po identyfikacji użytkownika, czyli po zadeklarowaniu swojej tożsamości, np. poprzez podanie loginu. Zadeklarowana ale jeszcze niezwerifikowana tożsamość jest potwierdzana w procesie uwierzytelnienia, np. poprzez podanie hasła, numeru PIN.
 - Użytkowników Zasobów IT Przemysłowego należy uwierzytelniać za pomocą odpowiednich metod uwierzytelniania, którymi mogą być:
 - Hasła statyczne – „coś co wiesz”, sekwencje liter, cyfr i znaków specjalnych (!, @, &, ^, +, #, itp.)
 - Hasła jednorazowe – „coś co masz”, hasło jednorazowe jest wykorzystywane tylko raz i traci ważność po wykorzystaniu lub po upływie określonego czasu ważności
 - Certyfikaty – uwierzytelnianie w oparciu o dowód posiadania klucza prywatnego
 - Dwuskładnikowe uwierzytelnienie – jest kombinacją opisanych powyżej metod uwierzytelniania.

5.0 Zarządzanie dostępem do Zasobów Przemysłowych

- Dopuszczalne jest użycie następujących typów kont:
 - Konta techniczne
 - Konta techniczne (Runtime)
 - Konta serwisowe
 - Konta administracyjne
 - Konta współdzielone
- Wszystkie identyfikatory (konta) wykorzystywane do uwierzytelniania w Zasobach IT Przemysłowego muszą być zinwentaryzowane. Za inwentaryzację kont odpowiada Zespół IT Przemysłowego
- Nazwy kont w Systemach Przemysłowych powinny być nadawane zgodnie z przyjętą konwencją nazewnictwa, która umożliwia jednoznaczną identyfikację użytkownika lub w przypadku kont nieimiennych, przeznaczenie konta
- W Systemach Przemysłowych, działania realizowane przez użytkowników muszą być rozliczane i być jednoznacznie przypisane do danego użytkownika. Wyjątkiem są Konta Techniczne, Konta Techniczne (Runtime), Konta Serwisowe, Konta Współdzielone
- Każde Konto Współdzielone lub Konto Serwisowe musi być zarejestrowane w manager'ze haseł
- Konta typu „gość” zaimplementowane w Zasobach IT Przemysłowego powinny być usunięte lub zablokowane
- Domyślne konta generowane podczas instalacji Systemu Przemysłowego powinny zostać usunięte lub zablokowane, jeśli jest to technicznie możliwe
- Wszystkie hasła do Zasobów IT Przemysłowego, niebędące hasłami indywidualnych użytkowników powinny być zapisane i zabezpieczone w fizycznych lub elektronicznych sejfach, a dostęp do nich ograniczony
- Wszystkie domyślne hasła muszą zostać zmienione
- Konta techniczne
 - Wykorzystywanie Kont Technicznych jest dopuszczalne wyłącznie na potrzeby uwierzytelniania na poziomie system-system lub usługa-usługa. Niedopuszczalne jest używanie Kont Technicznych przez użytkowników do uwierzytelniania w Zasobach IT Przemysłowego. W przypadku wykorzystania Kont Technicznych należy:
 - Zarejestrować nazwy Kont Technicznych i hasła w menedżerze haseł
 - Wyłączyć mechanizm okresowej zmiany hasła w przypadku kont domenowych
 - Wyłączyć funkcję pojedynczego logowania (z ang. Single Sign-on) do innych Zasobów IT Przemysłowego w przypadku kont domenowych
 - Wszystkie Konta Techniczne – jeśli są niezbędne do poprawnej pracy Zasobów IT Przemysłowego – muszą zostać pozyskane od dostawców i przekazane do Zespołu IT Przemysłowego, a domyślne hasła zmienione zgodnie z obowiązującą polityką haseł.

- Konta Techniczne (Runtime)
 - Wykorzystanie Kont Technicznych (Runtime) dopuszczalne jest na potrzeby uwierzytelniania system – system / usługa - usługa oraz na potrzeby wprowadzania zmian w Systemach Przemysłowych przez Zespół IT Przemysłowego i dostawców. Należy stosować następujące zasady bezpieczeństwa:
 - Zarejestrować nazwy Kont Technicznych (Runtime) i haseł w menedżerze haseł
 - Wyłączyć mechanizm okresowej zmiany hasła w przypadku kont domenowych
 - Wyłączyć funkcję pojedynczego logowania (z ang. Single Sign-on) do innych Zasobów IT Przemysłowego, w przypadku kont domenowych
 - Zmienić domyślną nazwę konta i hasło, jeśli jest to technicznie możliwe
- Konta Serwisowe
 - Wykorzystanie Kont Serwisowych dopuszczalne jest na potrzeby Zespołu IT Przemysłowego oraz dostawców w celu wykonania prac rozwojowych lub utrzymaniowych na poziomie systemu operacyjnego. Należy stosować następujące zasady bezpieczeństwa:
 - Zarejestrować nazwy Kont Serwisowych i haseł w menedżerze haseł
 - Wyłączyć mechanizm okresowej zmiany hasła
 - Wyłączyć funkcję pojedynczego logowania (z ang. Single Sign-on) do innych Zasobów IT Przemysłowego, w przypadku kont domenowych
- Konta Administracyjne
 - Konta imienne z uprawnieniami uprzywilejowanymi zarejestrowane w usłudze katalogowej (Active Directory) wykorzystywane są przez dostawców w następujących celach:
 - W celu zestawienia tunelu VPN client-site z infrastrukturą QEMETICA
 - W celu zestawienia sesji do docelowych Zasobów IT Przemysłowego przy użyciu systemu klasy PAMNależy stosować następujące zasady bezpieczeństwa:
 - Wszystkie Konta Administracyjne muszą być zinwentaryzowane
 - Niedopuszczalne jest udostępnianie Kont Administracyjnych innym użytkownikom, niż tym do których zostały one indywidualnie przypisane
 - Niedopuszczalne jest użycie Kont Administracyjnych do uwierzytelniania na poziomie system-system / usługa-usługa
 - Przy nadawaniu dostępów i uprawnień należy stosować zasadę najmniejszych uprawnień
 - Ważność kont musi być przedłużana co 3 miesiące
 - Hasła do kont muszą być zmieniane co 2 miesiące
 - Konta imienne z uprawnieniami uprzywilejowanymi wykorzystywane przez Zespół IT Przemysłowego do prac rozwojowych, utrzymaniowych i serwisowych na zasobach zarejestrowanych w usłudze katalogowej (Active Directory). Należy stosować następujące zasady bezpieczeństwa:
 - Wszystkie Konta Administracyjne muszą być zinwentaryzowane
 - Niedopuszczalne jest udostępnianie Kont Administracyjnych innym użytkownikom, niż tym do których zostały one indywidualnie przypisane
 - Niedopuszczalne jest użycie Kont Administracyjnych do uwierzytelniania na poziomie system-system / usługa-usługa
 - Przy nadawaniu dostępów i uprawnień należy stosować zasadę najmniejszych uprawnień

- Konta Współdzielone
 - Wykorzystanie Kont Współdzielonych dopuszczalne jest na potrzeby uwierzytelniania do Systemów Przemysłowych z poziomu Cienkiego Klienta do Stacji Operatorskich lub Stacji Inżynierskich. Należy stosować następujące zasady bezpieczeństwa:
 - Wszystkie Konta Współdzielone muszą być zinwentaryzowane
 - Zarejestrować nazwy Kont Współdzielonych i haseł w menedżerze haseł
 - Konta Współdzielone i hasła powinny być zaszyte w skryptach logujących Użytkownika do Systemów Przemysłowych

6.0 Redundancja Systemów i Infrastruktury IT Przemysłowego

- W celu zapewnienia ciągłości procesu sterowania i nadzoru nad procesami technologicznymi, niezbędne jest zapewnienie redundancji na poziomie:
 - Infrastruktury sieciowej
 - Przełączniki dostępowe
 - Przełączniki przemysłowe
 - Infrastruktury sprzętowej
 - Serwery przemysłowe
 - Stacje operatorskie
 - Stacje inżynierskie

7.0 Bezpieczeństwo Systemów IT Przemysłowego

- Dostawca DCS zapewni, że cały system sterowania stacje robocze i serwery będą skonfigurowane tak, aby zapewniały wszystkim użytkownikom najniższe uprawnienia konfiguracyjne oraz aby system sterowania nie wymagał kont użytkowników o wysokim poziomie uprawnień do wykonywania standardowych czynności wykonawczych.
- Warstwa systemu operacyjnego i warstwa aplikacyjna muszą być wspierane przez producenta, dostarczone w najwyższej dostępnej wersji wraz z zainstalowanymi aktualizacjami i poprawkami bezpieczeństwa.
- Wszystkie biblioteki programistyczne, dodatki wykorzystane do tworzenia Systemu muszą być wspierane i rozwijane, co jest rozumiane jako spełnienie warunku wydania nowej wersji lub poprawki w ciągu ostatnich 6 miesięcy od momentu rozpoczęcia prac nad Systemem. W przypadku braku spełnienia tego warunku należy przedstawić oświadczenie producenta o zapewnieniu wsparcia i rozwoju.
- System IT Przemysłowego musi zostać dostarczony wraz z mapą ruchu sieciowego.

- System IT Przemysłowego musi zostać umieszczony w oddzielnym VLAN.
- System IT Przemysłowego musi zostać wdrożony z uwzględnieniem modelu segmentacji sieci w Grupie QEMETICA. Wymiana danych pomiędzy Systemami IT Przemysłowego, a innymi systemami informatycznymi musi odbywać się z zachowaniem modelu segmentacji sieci.
- System operacyjny na którym zostanie zainstalowany System IT Przemysłowego musi umożliwiać instalację klienta Microsoft Defender for Endpoint.
- Procesy Systemu Przemysłowego, które będą korzystać z procesu LSASS muszą zostać jasno wskazane przez Dostawcę w celu dodania komponentu do wyjątków w ramach reguł bezpieczeństwa.
- System IT Przemysłowego powinien umożliwiać integrację z AD na poziomie uwierzytelniania i obsługiwać mechanizm SSO. W przypadku braku integracji z AD, System musi posiadać politykę zarządzania hasłami i własne mechanizmy uwierzytelniania.
- System IT Przemysłowego nie może się komunikować z żadnymi zewnętrznymi źródłami, usługami chmurowymi.
- Dostęp do zasobów Internet z Systemów IT Przemysłowego lub dowolnego komponentu podłączonego do sieci przemysłowej jest zabroniony.
- Systemy IT Przemysłowego nie mogą być wystawione do sieci publicznej.
- Niezbędne jest wyłączenie niewykorzystanych usług, protokołów, interface'ów sieciowych.

8.0 Bezpieczeństwo Stacji Inżynierskich

- Dostęp do stacji inżynierskich musi być uwierzytelniany przy użyciu imiennych poświadczeń domenowych lub imiennych poświadczeń lokalnych.
- Stacje inżynierskie nie mogą mieć dostępu do zasobów sieci Internet.
- Bezpośredni dostęp do stacji inżynierskich z poziomu sieci IT jest zabroniony.
- Stacje inżynierskie muszą się znajdować w wydzielonych fizycznych strefach bezpieczeństwa, niedostępnych dla osób postronnych.

9.0 Bezpieczeństwo Stacji Operatorskich

- Dostęp do stacji operatorskich musi być uwierzytelniany przy użycia imiennych poświadczeń domenowych lub imiennych poświadczeń lokalnych lub kont współdzielonych.
- Stacje operatorskie nie mogą mieć dostępu do zasobów sieci Internet.
- Bezpośredni dostęp do stacji operatorskich z poziomu sieci IT jest zabroniony.
- Stacje inżynierskie muszą się znajdować w wydzielonych fizycznych strefach bezpieczeństwa, niedostępnych dla osób postronnych.

10.0 Zdalny dostęp

- Dostęp pracowników dostawców zewnętrznych do Zasobów IT Przemysłowego określają następujące zasady:
 - Dostęp do Zasobów IT Przemysłowego jest możliwy jedynie po podpisaniu stosownej umowy, która ściśle definiuje zasady dostępu, zakres i czas dostępu
 - Zawierana umowa musi zawierać wykaz dostęp wymaganych usług, wymagane środki bezpieczeństwa organizacyjnego i technicznego po stronie dostawcy zewnętrznego, oczekiwany poziom usług, oświadczenie o zachowaniu poufności, zasady współpracy w przypadku incydentów związanych z bezpieczeństwem oraz mechanizmy umożliwiające kontrolę i wgląd we wszystkie aspekty związane z bezpieczeństwem
 - Zakres dostępu dostawców zewnętrznych do Zasobów IT Przemysłowego powinien być ograniczony wyłącznie do tych zasobów, do których dostęp jest niezbędny do realizacji umowy i który został określony w umowie
 - Usługi świadczone przez Dostawców Zewnętrznych podlegają monitorowaniu i przeglądom w celu weryfikacji zgodności z zawartą umową o dostępie zdalnym.
- Zdalny dostęp do Systemów IT Przemysłowego możliwy jest jedynie poprzez centralny punkt styku z siecią publiczną.
- Niedopuszczalne jest stosowanie lokalnych rozwiązań do zdalnego dostępu na poziomie lokalizacji przemysłowej.
- Zdalny dostęp dostawców do Systemów IT Przemysłowego możliwy jest jedynie z wykorzystaniem koncentratora VPN i dwuskładnikowego

uwierzytelniania oraz systemu klasy PAM (z ang. Privileged Access Management), umożliwiającego zarządzanie i monitorowanie dostępu uprzywilejowanego.

- Zdalny dostęp Dostawców do Systemów IT Przemysłowego musi być realizowany przy zablokowanym dostępie do Internetu.
- Zdalny dostęp pracowników IT, IT Przemysłowego do Systemów IT Przemysłowego możliwy będzie jedynie przy użyciu zestawionego z infrastrukturą QEMETICA tunelu VPN.