

Obszar Informatyki PKN ORLEN SA

PKN ORLEN SA



Zestawienie standardowych zapisów dla postępowań inwestycyjnych w zakresie cyberbezpieczeństwa dla systemów Automatyki ICS - OT.

Dla nowobudowanych instalacji i procesu modernizacji
systemów automatyki ICS - OT

Zespół Bezpieczeństwa Systemów Automatyki Przemysłowej

Dokument ten definiuje standardowe zapisy, które muszą być zawarte podczas przygotowania zakresów prac modernizacji i budowy instalacji – w zakresie automatyki przemysłowej. Dotyczy to min. zapisów w zakresie wymaganej dokumentacji cyberbezpieczeństwa, minimalnych wymagań dla systemów OT oraz zapisów umownych w kontraktach.

Jakiegokolwiek zmiany w poniższych wymaganiach muszą być zaakceptowane przez Dział Bezpieczeństwa IT.

Termin "ICS" (skrót ICS oznacza przemysłowe systemy sterowania min. systemy monitorowania, zabezpieczania i kontroli przemysłowej) należy interpretować w rozumieniu systemów monitorowania, sterowania i bezpieczeństwa infrastruktury przemysłowej (wszystkie stacje PC, serwery, sterowniki PLC, kontrolery, urządzenia sieciowe, specjalistyczne oprogramowanie urządzeń).

I. Zapisy dotyczące dokumentów zawierających zakresy zleczanych prac (SIWZ):

1. Zakres prac związanych z systemami automatyki przemysłowej - Wykonawca wykona wszelkie prace oraz dostarczy rozwiązania niezbędne do wypełnienia zapisów standardu GK ORLEN „Podstawowe wymagania cyberbezpieczeństwa dla systemów automatyki ICS – OT” (w **Załącznik_1** „Wymagania cyberbezpieczeństwa - PKN ORLEN, Cyber security requirements - ORLEN CG”)
2. Zakres prac związanych z systemami automatyki przemysłowej - Wykonawca dostarczy dokumentację spełniającą wymagania w zakresie standardów dokumentacji cyberbezpieczeństwa (w **Załącznik_2** „Dokumentacja konfiguracyjna cyberbezpieczeństwa”)

II. Zapisy dotyczące umów z Wykonawcami:

1) § ... Zakres prac

W przypadku realizacji prac związanych z systemami automatyki przemysłowej Wykonawca w ramach Umowy wykona wszelkie prace oraz dostarczy rozwiązania niezbędne do wypełnienia zapisów standardu PKN ORLEN „Podstawowe wymagania cyberbezpieczeństwa dla systemów automatyki ICS – OT” oraz dostarczy dokumentację spełniającą wymagania w zakresie standardów cyberbezpieczeństwa „Dokumentacja konfiguracyjna cyberbezpieczeństwa” (**Załącznik_1**, **Załącznik_2**)

2) § ... Bezpieczeństwo teleinformatyczne

- 1) Wykonawca zobowiązuje się do wykonania przedmiotu Umowy przestrzegając zasad bezpieczeństwa teleinformatycznego określonych w Umowie.
- 2) Wykonawca zobowiązany jest posiadać politykę bezpieczeństwa teleinformatycznego, która ma wyraźne zastosowanie do usług świadczonych w ramach niniejszej Umowy.
- 3) Wykonawca zobowiązany jest zapewnić, że zarządzanie infrastrukturą teleinformatyczną wykorzystywaną do realizacji przedmiotu Umowy jest prowadzone zgodnie z dobrymi, uznanymi praktykami bezpieczeństwa teleinformatycznego.
- 4) W przypadku uzasadnionej konieczności Zamawiający udzieli upoważnionym osobom ze strony Wykonawcy dostępu logicznego (wyłącznie z wewnętrznej sieci teleinformatycznej) lub fizycznego do zasobów teleinformatycznych Zamawiającego na zasadach opisanych w dokumencie Bezpieczeństwo Teleinformatyczne – dostęp fizyczny i logiczny (**Załącznik_3** Zasady dostępu do zasobów teleinformatycznych Zamawiającego – dostęp fizyczny i logiczny).
- 5) W przypadku uzasadnionej konieczności Zamawiający może udzielić zdalnego dostępu do zasobów teleinformatycznych Zamawiającego. Warunkiem koniecznym do udzielenia zdalnego dostępu jest podpisanie przez Wykonawcę porozumienia VPN będącego standardem PKN ORLEN znajdującym się w dokumencie Porozumienie o zdalnym dostępie do zasobów teleinformatycznych (**Załącznik_4** – Wzór Porozumienia o zdalnym dostępie do zasobów teleinformatycznych Site-to-Site-NOWE, Wzór Porozumienia o zdalnym dostępie do zasobów teleinformatycznych).
- 6) Wykonawca zobowiązuje się do niezwłocznego powiadamiania Zamawiającego o zaistniałych naruszeniach lub incydentach bezpieczeństwa teleinformatycznego w związku z udzielonym dostępem do zasobów teleinformatycznych Zamawiającego.
- 7) Wykonawca zobowiązuje się do wykonywania obowiązków wynikających z Umowy w sposób zapobiegający utracie poufności, integralności i dostępności danych. W przypadku, gdy wykonanie Umowy wiąże się z ryzykiem utraty ww. atrybutów bezpieczeństwa danych, Wykonawca zobowiązany jest poinformować o tym Zamawiającego przed

przystąpieniem do wykonywania jakichkolwiek prac oraz umożliwić Zamawiającemu przeprowadzenie działań zapewniających zachowanie ww. atrybutów.

- 8) W sprawach określonych w niniejszym paragrafie oraz w Załącznikach do niniejszej Umowy Wykonawca odpowiada za skutki działań pracowników oraz osób trzecich, którym powierzył wykonanie czynności na rzecz Zamawiającego tak, jak za czynności własne.
- 9) W przypadku naruszenia przez Wykonawcę zasad bezpieczeństwa teleinformatycznego, Zamawiający może żądać zapłaty przez Wykonawcę kary umownej w wysokości 100.000 zł (słownie: sto tysięcy złotych) za każdy przypadek naruszenia. Uprawnienie do żądania kary umownej nie wyłącza uprawnienia Zamawiającego do dochodzenia odszkodowania uzupełniającego na zasadach ogólnych, w przypadku, gdy wysokość poniesionej szkody przewyższa zastrzeżoną wysokość kary umownej.
- 10) W przypadku decyzji Zamawiającego o wykonaniu weryfikacji cyberbezpieczeństwa (między innymi testów penetracyjnych) aplikacji lub systemów (w tym internetowych) służących do realizacji Umowy lub aplikacji lub systemu będącego przedmiotem Umowy, Kontrahent umożliwi taką weryfikację i w przypadku zidentyfikowania podatności zastosuje się do rekomendacji Zamawiającego.
- 11) Wykonawca zapewni, że aplikacje internetowe, służące do realizacji przedmiotu Umowy i aplikacje lub system będące przedmiotem Umowy:
 - (a) będą zbudowane zgodnie z przekazanym lub udostępnionym Kontrahentowi Regulaminie pt. „Wymaganiami bezpieczeństwa dla budowy bezpiecznych aplikacji w PKN ORLEN S.A.” w zakresie, w jakim odnoszą się do przedmiotu Umowy;
 - (b) będą funkcjonowały zgodnie z uznanym międzynarodowymi standardami w zakresie bezpieczeństwa aplikacji internetowymi takimi, jak np. OWASP;
 - (c) nie będą podatne na typowe zagrożenia z sieci Internet (OWASP Top Ten).

3) § ... Praca odbiorowe w zakresie cyberbezpieczeństwa

- 1) Kontrahent zobowiązany jest do zgłoszenia gotowości do odbioru systemu w zakresie cyberbezpieczeństwa najpóźniej na 2 tygodnie przed planowanym terminem odbioru.
- 2) Wymagane jest przekazanie finalnej dokumentacji systemowej (min. spełniającej wymagania w zakresie standardów dokumentacji cyberbezpieczeństwa (Załącznik_2 „Dokumentacja konfiguracyjna cyberbezpieczeństwa”) oraz innych dokumentów odbiorowych (m.in. protokół przekazania licencji, lista wszystkich kont/grup użytkowników, procedura wykonywania/odtworzenia backupów, backup plan, dokumentacja funkcjonalna systemu) umożliwiających przeprowadzenie odbioru, nie później niż 4 dni przed ich rozpoczęciem.
- 3) *Dostawca* zapewni środowisko umożliwiające przeprowadzenie testów *odbiorowych*
- 4) Po usunięciu usterki zalecane jest powtórne wykonanie testu w zakresie zgłoszonej usterki.