



Aneks nr 1 z dnia 21.09.2026r. do Specyfikacji Nr OI-1/14/2026 z dnia 21.08.2026r.

dotyczy: Modernizacja systemu wizualizacji, wymiana stacji komputerowych systemu Scada oraz zaprojektowanie i budowa nowego pomieszczenia dla serwerowni w KS Mogilno.

Obowiązuje
z dniem zatwierdzenia

Niniejszym aneksem zmianie ulega zapis pkt. VI specyfikacji Nr OI-1/14/2026 z dnia 21.08.2026r.

VI. Rysunki, wzory, załączniki:

- a. Dokument potwierdzający przekazanie odpadów niebezpiecznych do ostatecznego procesu (zał. nr 1).
- b. Podstawowe wymagania cyberbezpieczeństwa dla systemów ICS-OT (zał. nr 2).
- c. Wymagania bezpieczeństwa (ogólne) na etapie RFI (zał. nr 3).
- d. Bezpieczeństwo teleinformatyczne – dostęp fizyczny i logiczny do systemów OT (zał. nr 4).

i otrzymuje następujące brzmienie:

VI. Rysunki, wzory, załączniki:

- a. Podstawowe wymagania cyberbezpieczeństwa dla systemów automatyki ICS-OT (zał. nr 1.1 Wytyczne techniczne Cyberbezpieczeństwa OT do zakupów i inwestycji)
- b. Podstawowe wymagania cyberbezpieczeństwa dla systemów automatyki ICS-OT (zał. nr 1.1.1 Dokumentacja konfiguracyjna cyberbezpieczeństwa OT)
- c. Podstawowe wymagania cyberbezpieczeństwa dla systemów automatyki ICS-OT (zał. nr 1.1.2 Aktualna Konfiguracja Cyberbezpieczeństwa OT)
- d. Podstawowe wymagania cyberbezpieczeństwa dla systemów automatyki ICS-OT (zał. nr 1.1.3 Procedura Zarządzania Logami Cyberbezpieczeństwa OT)
- e. Podstawowe wymagania cyberbezpieczeństwa dla systemów automatyki ICS-OT (zał. nr 1.1.4 Architektura OT)
- f. Podstawowe wymagania cyberbezpieczeństwa dla systemów automatyki ICS-OT (zał. nr 1.1.5 Dokumentacja konfiguracyjna cyberbezpieczeństwa OT – Arkusz z danymi)
- g. Podstawowe wymagania cyberbezpieczeństwa dla systemów automatyki ICS-OT (zał. nr 2.1 Zasady Bezpieczeństwa Teleinformatycznego OT)
- h. Podstawowe wymagania cyberbezpieczeństwa dla systemów automatyki ICS-OT (zał. nr 1.3 Bezpieczeństwo teleinformatyczne – dostęp fizyczny i logiczny OT)
- i. Podstawowe wymagania cyberbezpieczeństwa dla systemów automatyki ICS-OT (zał. nr 1.4 Porozumienie o udostępnieniu zdalnego dostępu do zasobów teleinformatycznych)

j. Dokument potwierdzający przekazanie odpadów niebezpiecznych do ostatecznego procesu (zł. nr 1.5) .

oraz dodano niniejszym aneksem do Specyfikacji Nr OI-1/14/2026 z dnia 21.08.2026r. pkt. XI Wytyczne cyberbezpieczeństwa OT do zakupów i inwestycji w Orlen S.A.

- 1) W przypadku realizacji prac związanych z systemami ICS / OT Wykonawca w ramach Umowy zobowiązuje się do wykonania przedmiotu Umowy przestrzegając zasad bezpieczeństwa teleinformatycznego określonych w Umowie, wykona wszelkie prace oraz dostarczy rozwiązania niezbędne do wypełnienia wymagań ORLEN S.A. w zakresie cyberbezpieczeństwa OT / ICT zawartych w:
 - a. Zał. 1.1 *Wytyczne techniczne Cyberbezpieczeństwa do zakupów i inwestycji*
 - b. Zał. 1.2 *Zasady Bezpieczeństwa Teleinformatycznego OT*
 - c. Standardach międzynarodowych IEC 62443, ISO 27001, ISO 22301, zakładając, że różnice pomiędzy standardami ORLEN S.A. a standardami międzynarodowymi wynikają ze specyfiki operacyjnej Spółki, to standardy ORLEN S.A. mają pierwszeństwo w zastosowaniu.
 - d. Wymogach prawnych obowiązujących na terenie Unii Europejskiej oraz Polski w tym między innymi:
 - Ustawa o Krajowym Systemie Cyberbezpieczeństwa (UKSC) „USTAWA z dnia 5 lipca 2018 r. o krajowym systemie Cyberbezpieczeństwa” dziennik ustaw 2018/1560 wraz nowelizacją uwzględniając również propozycje nowelizacji ustawy z dnia 2 grudnia 2024 r.
 - Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2557 z dnia 14 grudnia 2022 r. w sprawie odporności podmiotów krytycznych i uchylająca dyrektywę Rady 2008/114/WE
 - Rekomendacje Ministra Klimatu i Środowiska dotyczące działań mających na celu wzmocnienie cyberbezpieczeństwa w sektorze energii oraz wytyczne sektorowe dotyczące zgłaszania incydentów, Warszawa wrzesień 2021 r.
 - e. Wymogach wewnętrznych ORLEN S.A., które opierają się na scentralizowanym zarządzaniu cyberbezpieczeństwem w obszarach IT/OT, ważne jest, aby przy projektowaniu, wdrażaniu lub dostarczaniu rozwiązań z zakresu cyberbezpieczeństwa uwzględniać scentralizowany model zarządzania cyberbezpieczeństwem ORLEN S.A..
- 2) W przypadku implementowania/dostarczania aplikacji Wykonawca zobligowany jest do spełnienia wymagań zawartych w *Wymagania cyberbezpieczeństwa dla budowy bezpiecznych aplikacji w ORLEN S.A.* Zamawiający może udzielić odstępstwa od spełnienia wymagania zawartego w niniejszym punkcie na prośbę Wykonawcy.
- 3) Wykonawca zobowiązuje się do wykonania przedmiotu Umowy, przestrzegając zasad bezpieczeństwa teleinformatycznego określonych w Umowie.
- 4) Wykonawca zobowiązany jest posiadać politykę bezpieczeństwa teleinformatycznego, która ma wyrażać zastosowanie do usług świadczonych w ramach niniejszej Umowy.
- 5) Wykonawca zobowiązany jest zapewnić, że zarządzanie infrastrukturą teleinformatyczną wykorzystywaną do realizacji przedmiotu Umowy jest prowadzone zgodnie z dobrymi, uznanymi praktykami bezpieczeństwa teleinformatycznego.
- 6) W przypadku uzasadnionej konieczności Zamawiający może udzielić upoważnionym osobom ze strony Wykonawcy dostępu logicznego (wyłącznie z wewnętrznej sieci teleinformatycznej) lub fizycznego do zasobów teleinformatycznych Zamawiającego na zasadach opisanych w Zał. 1.3 Bezpieczeństwo teleinformatyczne - dostęp fizyczny i logiczny_OT. Warunkiem koniecznym do udzielenia dostępu jest:
 - a. przekazanie akceptacji przez obszar odpowiedzialny za realizację umowy po stronie Zamawiającego na realizację dostępu logicznego lub dostępu fizycznego do przedstawiciela obszaru cyberbezpieczeństwa ORLEN,

- b. przekazanie i akceptację przez obszar odpowiedzialny za realizację umowy po stronie Zamawiającego do obszaru cyberbezpieczeństwa ORLEN wykazu osób ze strony Wykonawcy upoważnionych do dostępu logicznego do zasobów teleinformatycznych z wewnętrznej sieci teleinformatycznej Zamawiającego oraz zakresu dostępu Zał. 1.3 Bezpieczeństwo teleinformatyczne - dostęp fizyczny i logiczny_OT,
- c. uzyskanie akceptacji przedstawiciela obszaru cyberbezpieczeństwa ORLEN.
- 7) W przypadku uzasadnionej konieczności Zamawiający może udzielić zdalnego dostępu do zasobów teleinformatycznych Zamawiającego na warunkach opisanych w Zał. 1.4 Porozumienie o udostępnieniu zdalnego dostępu do zasobów teleinformatycznych. Warunkiem koniecznym do udzielenia zdalnego dostępu jest:
- a. przekazanie akceptacji na realizację zdalnego dostępu do Przedstawiciela Zamawiającego w zakresie Zdalnego Dostępu przez obszar odpowiedzialny za realizację umowy po stronie Zamawiającego,
- b. Przekazanie przez obszar odpowiedzialny za realizację umowy po stronie Zamawiającego do Przedstawiciela Zamawiającego w zakresie Zdalnego Dostępu i akceptacja **Zakresu Zdalnego Dostępu i Listy Osób Uprawnionych** - Zał. 1.4 Porozumienie o udostępnieniu zdalnego dostępu do zasobów teleinformatycznych,
- c. Uzyskanie akceptacji przedstawiciela obszaru cyberbezpieczeństwa ORLEN.
- 8) Wykonawca zobowiązuje się do niezwłocznego powiadomiania Zamawiającego o zaistniałych naruszeniach lub incydentach bezpieczeństwa teleinformatycznego w związku z udzielonym dostępem do zasobów teleinformatycznych Zamawiającego.
- 9) 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 zapobiegających zachowanie ww. atrybutów.
- 10) 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.
- 11) 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.
- 12) 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.
- 13) Wykonawca zapewni, że aplikacje internetowe, służące do realizacji przedmiotu Umowy i aplikacje lub systemy będące przedmiotem Umowy:
- a. będą zbudowane zgodnie z przekazanym lub udostępnionym Kontrahentowi Regulaminem pt. „Wymagania cyberbezpieczeństwa dla budowy aplikacji w ORLEN S.A.” w zakresie, w jakim odnoszą się do przedmiotu Umowy;
- b. będą funkcjonowały zgodnie z uznanymi międzynarodowymi standardami w zakresie bezpieczeństwa aplikacji internetowych, takimi jak np. OWASP;
- c. nie będą podatne na typowe zagrożenia z sieci Internet (OWASP Top Ten).

TABELE ZATWIERDZEŃ I AKTUALIZACJI:

Opracował PC :	Sprawdził : OI-1	Zatwierdził:
Szymon Skorski Pełnomocnik ds. cyberbezpieczeństwa	Kierownik Działu Inwestycji i Remontów Rafał Męczyński	Rafał Braszkievicz Dyrektor ds. Inwestycji
Data: 21.09.2026 Podpis: 	Data: 21.09.2026 Podpis: 	Data: 21.09.2026 Podpis: 

AKTUALIZACJA:

Aktualizował :	Aktualizował :	Aktualizował :	Aktualizował :
Data: Podpis:	Data: Podpis:	Data: Podpis:	Data: Podpis: