

Wymagania Cyberbezpieczeństwa, Poufności, Ochrony Danych oraz Odpowiedzialność Podmiotów Trzecich zgodnie z wymogami OSE/OUK, a także Wymagania zgodności z UKSC i NIS2.

1. **Wykonawca zobowiązuje się** do pełnego przestrzegania wymogów wynikających z ustawy z dnia 5 lipca 2018 r. o Krajowym Systemie Cyberbezpieczeństwa, dyrektywy NIS2, RODO oraz wszystkich regulacji, standardów i procedur bezpieczeństwa obowiązujących u Operatora Usług Kluczowych (Zamawiającego), w tym polityk bezpieczeństwa informacji, polityk OT/ICS, instrukcji ruchu i eksploatacji oraz wytycznych dotyczących ochrony infrastruktury krytycznej.
2. W przypadku gdy realizacja umowy obejmuje dostęp do systemów, danych, urządzeń lub infrastruktury stanowiącej **usługę kluczową, infrastrukturę krytyczną, infrastrukturę OT/ICS, SCADA**, systemy sterowania, telemechaniki, pomiarów, automatyki zabezpieczeniowej lub systemów wspierających ich działanie, Wykonawca zobowiązuje się do stosowania środków bezpieczeństwa zgodnych z wymaganiami OSE, w tym standardów **IEC 62443, ISO 27019, ISO 27001** oraz wytycznych branżowych dla energetyki.
3. Wykonawca zobowiązuje się do korzystania z zasobów Zamawiającego wyłącznie zgodnie z obowiązującymi procedurami bezpieczeństwa, w szczególności dotyczącymi:
 - **zdalnego dostępu wyłącznie poprzez autoryzowane połączenia VPN,**
 - stosowania **MFA/silnego uwierzytelniania,**
 - stosowania zasady **least privilege,**
 - segmentacji sieci i separacji środowisk OT/IT,
 - rejestrowania i monitorowania aktywności użytkowników.
4. Wykonawca zapewnia, że wszelkie dane przetwarzane w związku z realizacją umowy, w tym dane techniczne dotyczące infrastruktury energetycznej, dane operacyjne, dane pomiarowe, dane osobowe oraz dane dotyczące usług kluczowych, będą chronione poprzez:
 - **szyfrowanie danych w spoczynku i w transmisji,**
 - kontrolę dostępu i zarządzanie tożsamością,
 - aktualizacje bezpieczeństwa i zarządzanie podatnościami,
 - stosowanie zabezpieczeń chroniących przed ingerencją w systemy OT/ICS.
5. Wykonawca zobowiązuje się do prowadzenia **rejestracji i logowania dostępu** do systemów, danych i zasobów Zamawiającego, w sposób umożliwiający identyfikację użytkownika, czasu, zakresu oraz charakteru wykonanych operacji. Logi muszą być przechowywane zgodnie z wymaganiami OSE, w sposób uniemożliwiający ich modyfikację lub usunięcie.
6. Wykonawca zobowiązuje się do wykonywania **regularnych kopii zapasowych (backupów)** danych, konfiguracji systemów oraz środowisk wykorzystywanych w ramach realizacji umowy, zgodnie z wymaganiami Zamawiającego oraz standardami branżowymi, w sposób zapewniający możliwość odtworzenia danych po incydencie.
7. W przypadku wystąpienia **incydentu cyberbezpieczeństwa**, naruszenia ochrony danych osobowych, zakłócenia działania systemów OT/ICS, podejrzenia naruszenia poufności lub

integralności danych, bądź jakiegokolwiek zdarzenia mogącego mieć wpływ na ciągłość świadczenia usługi kluczowej, Wykonawca zobowiązuje się do:

- niezwłocznego poinformowania Zamawiającego, nie później niż w ciągu **4 godzin**,
 - podjęcia działań minimalizujących skutki incydentu,
 - pełnej współpracy przy analizie, raportowaniu i usuwaniu skutków incydentu,
 - przekazania Zamawiającemu pełnej dokumentacji zdarzenia, w tym logów, danych technicznych i informacji operacyjnych,
 - wsparcia Zamawiającego w realizacji obowiązków raportowych wobec CSIRT.
8. Wykonawca zobowiązuje się umożliwić Zamawiającemu lub upoważnionym przez niego podmiotom przeprowadzenie **audytów bezpieczeństwa**, kontroli zgodności, testów penetracyjnych, audytów OT/ICS oraz przeglądów technicznych dotyczących realizacji umowy. Wykonawca zobowiązuje się do pełnej współpracy oraz wdrożenia zaleceń wynikających z audytu w terminie wskazanym przez Zamawiającego.
9. Wykonawca zapewnia, że wszystkie osoby działające w jego imieniu, w tym pracownicy, współpracownicy, podwykonawcy oraz inne podmioty trzecie zaangażowane w realizację umowy, zostaną zapoznane z obowiązującymi procedurami bezpieczeństwa i będą ich przestrzegać. **Wykonawca ponosi pełną odpowiedzialność za działania i zaniechania tych podmiotów jak za własne**, w tym za wszelkie naruszenia poufności, procedur bezpieczeństwa, zasad dostępu do infrastruktury krytycznej oraz wymogów OSE.
10. W przypadku naruszenia obowiązków wynikających z niniejszego paragrafu, w tym naruszeń dokonanych przez podwykonawców lub inne podmioty trzecie, Wykonawca zapłaci Zamawiającemu **karę umowną w wysokości nie mniejszej niż 5% wartości kontraktu**, nie więcej jednak niż do wysokości **rzeczywiście poniesionych strat przez Zamawiającego**. Zapłata kary umownej nie wyłącza prawa Zamawiającego do dochodzenia odszkodowania uzupełniającego na zasadach ogólnych.

Zakończenie współpracy

11. Po zakończeniu umowy Wykonawca:
- usuwa dane Zamawiającego,
 - zwraca dokumentację,
 - potwierdza usunięcie danych protokołem.

Wymagania zgodności z UKSC i NIS2

- zgodnie z pkt. 6 SWZ.

.....
(miejscowość, data)

.....
(pieczęć i podpisy osób uprawnionych)