**Oświadczenie Wykonawcy**

Przystępując do udziału w postępowaniu o udzielenie zamówienia nr **RPUZ/P/0017/2026/OD/ZIR/RI**, którego przedmiotem jest **Modernizacja układu automatycznej regulacji napięcia transformatorów ARN** prowadzonego w trybie otwartymoświadczam, iż:

**…………………………………………………………………………………………………………………**

***(nazwa Wykonawcy)***

stosuje rozwiązania organizacyjne Systemu Zarządzania Bezpieczeństwem Informacji oparte o system zarządzania wg. PN-EN ISO/IEC 27001 oraz wyraża zgodę na weryfikację wymagań przez Zamawiającego.

Informuje o stosowaniu co najmniej następujących rozwiązań:

| **OBSZAR ROZWIĄZAŃ** |
| --- |
| **ORGANIZACYJNO-PRAWNY i ZASOBÓW LUDZKICH** |
| 1. Wprowadzono polityki/procedury/instrukcje zapewniające adekwatny poziom bezpieczeństwa. |
| 1. Przypisano odpowiedzialności w zakresie bezpieczeństwa do konkretnych ról/stanowisk/osób. |
| 1. Zamawiający zostanie poinformowany o incydencie naruszenia bezpieczeństwa, jeśli dotyczyć on będzie usług wykonywanych dla Zamawiającego. |
| 1. Stosuje się formalny program podnoszenia świadomości użytkowników w zakresie bezpieczeństwa (np. szkolenia). |
| 1. Formalnie klasyfikuje się informację i postępuje zgodnie z przyjętym poziomem jej ochrony. |
| 1. Mamy świadomość jakie usługi Zamawiającego mają być świadczone w określonych krytycznych ramach czasowych na wypadek katastrofy/awarii.  Dostawca/Wykonawca dba o aktualne procedury w sytuacjach awaryjnych. |
| 1. Umowy o zachowaniu poufności są podpisywane przed ujawnieniem informacji poufnych współpracownikom. |
| **TELEINFORMATYCZNY i FIZYCZNO-ŚRODOWISKOWY** |
| 1. Kontroluje się dostęp do bezpiecznych obszarów, np. zarządzanie dystrybucją kluczy (zarówno fizyczną, jak i elektroniczną), dzienniki papierowe/elektroniczne, monitorowanie drzwi obiektów, dostęp do serwerowni itp. |
| 1. Stosuje się systemy antywłamaniowe w miejscach przechowywania urządzeń zabezpieczeń i telemechaniki oraz IT na potrzeby realizacji zadania. |
| 1. Nie stosuje się podłączania niedozwolonych urządzeń bez zgody Zamawiającego do sieci LAN Zamawiającego (za wyjątkiem dostępu jako gość). |
| 1. Nie wykorzystuje się chmury publicznej (np. AWS, GCP, Azure) i publicznych zasobów plikowych (np. DropBox, Google Drive, OneDrive) do wykonywania zadań powierzonych przez Zamawiającego. |
| 1. Stosuje się ochronę przed wirusami, spamem i malware w systemach wykorzystywanych do realizacji zlecenia. |
| 1. Stosuje się zasadę nie korzystania z urządzeń prywatnych do celów służbowych. |
| 1. Stosuje się zasadę nie korzystania ze służbowy laptopów i urządzeń mobilnych, wykorzystywanych do realizacji zlecenia, do celów prywatnych. |
| 1. Przesyłając pliki z informacją chronioną szyfruje się je zabezpieczając możliwie silnym hasłem. Hasła do plików są przesyłane innym kanałem niż plik. |
| 1. Zabezpiecza się lub szyfruje poufne informacje na laptopach i urządzeniach mobilnych (partycje lub dyski). |
| 1. Systemy operacyjne i kluczowe aplikacje na wykorzystywanych urządzeniach posiadają ważne wsparcie producenta przynajmniej w okresie świadczenia usługi dla Zamawiającego. |
| 1. Niezwłocznie wdraża się krytyczne zabezpieczenia w celu ochrony przed podatnościami. |
| 1. Urządzenia i oprogramowanie, dostarczane w związku z realizacją zadania, zabezpieczone są przed dostępem osób trzecich na adekwatny poziomie do ryzyka ich kradzieży, modyfikacji lub podmiany, są fabrycznie nowe z najnowszą dostępną wersją oprogramowania firmware oraz oprogramowania systemowego, a tam gdzie to możliwe w oryginalnych nienaruszonych opakowaniach. |

|  |  |
| --- | --- |
|  |  |
| miejscowość i data | Podpis przedstawiciela(i) Wykonawcy |