

Oświadczenie Wykonawcy

Przystępując do udziału w postępowaniu o udzielenie zamówienia nr RPUZ/P/0913/2024/OD/RD-4, którego przedmiotem jest „ RD4 PE Śrem - Modernizacja pokrycia dachowego budynku garażowego PE” Zadanie realizowane w trybie otwartym oświadczam, iż:

(nazwa Wykonawcy)

stosuje rozwiązania organizacyjne Systemu Zarządzania Bezpieczeństwem Informacji oparte o system zarządzania wg. PN-EN ISO/IEC 27001:2017 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
2. Przypisano odpowiedzialności w zakresie bezpieczeństwa do konkretnych ról/stanowisk/osób
3. Będzie się informować Zamawiającego o incydencie naruszenia bezpieczeństwa, jeśli dotyczyć on będzie usług wykonywanych dla Zamawiającego
4. Stosuje się formalny program podnoszenia świadomości użytkowników w zakresie bezpieczeństwa (np. szkolenia)
5. Formalnie klasyfikuje się informację i postępuje z informacją zgodnie z przyjętym poziomem jej ochrony
6. 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.
7. 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.
2. Stosuje się systemy antywłamaniowe w miejscach przechowywania urządzeń zabezpieczeń i telemechaniki oraz IT na potrzeby realizacji zadania
3. Nie będzie się podłączać niedozwolonych urządzeń bez zgody Zamawiającego do sieci LAN Zamawiającego (za wyjątkiem dostępu jako gość)
4. Nie będą wykorzystywane chmury publiczne (np. AWS, GCP, Azure) i publiczne zasoby plikowe (np. DropBox, Google Drive, OneDrive) do wykonywania zadań powierzonych przez Zamawiającego
5. Stosuje się ochronę przed wirusami, spamem i malware w systemach wykorzystywanych do realizacji zlecenia
6. Stosuje się zasadę nie korzystania z urządzeń prywatnych do celów służbowych
7. Stosuje się zasadę nie korzystania ze służbowy laptopów i urządzeń mobilnych, wykorzystywanych do realizacji zlecenia, do celów prywatnych
8. Przesyłając pliki z informacją chronioną szyfruje się je zabezpieczając możliwie silnym hasłem. Hasła do plików są przysyłane innym kanałem niż plik.
9. Zabezpiecza się lub szyfruje poufne informacje na laptopach i urządzeniach mobilnych (partycje lub dyski)
10. Systemy operacyjne i kluczowe aplikacje na wykorzystywanych urządzeniach posiadają ważne wsparcie producenta przynajmniej w okresie świadczenia usługi dla Zamawiającego
11. Niezwłocznie wdraża się krytyczne zabezpieczenia w celu ochrony przed podatnościami
12. 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