Oława dnia 03.03.2025r.

Zamawiający:
PRZEDSIĘBIORSTWO KOMUNIKACJI SAMOCHODOWEJ W OŁAWIE S.A.
UL. OPOLSKA 50, 55 – 200 OŁAWA

Odpowiedzi na zapytania wykonawców dotyczące treści SWZ

Dotyczy: „Przygotowanie pełnej dokumentacji do audytu spełnienia wymogów związanych z bezpieczeństwem systemów informacyjnych wykorzystywanych do świadczenia usług kluczowych zgodnie z ustawą o krajowym systemie cyberbezpieczeństwa oraz dyrektywą NIS2"

Zamawiający udziela następujących odpowiedzi na pytania:

Pytania z dnia 24.02.2025

Czy przez przygotowanie dokumentacji SZBI zamawiający rozumie wykonanie następujących działań?
Wykonawca jest odpowiedzialny za przeprowadzenie wdrożenie kompletnego Systemu Zarządzania Bezpieczeństwem Informacji (dalej zwany: SZBI) dla Zamawiającego. Zakres audytu systemu bezpieczeństwa informacji każdorazowo obejmie zgodność z kryteriami zawartymi w § 19 ust. 2 ww. rozporządzenia KRI oraz zgodność z wymaganiami normy PN-EN ISO/IEC 27001:2023 dla Zamawiającego. Raport z audytu KRI zostanie każdorazowo podpisany przez audytora dokonującego audyt KRI przy wykorzystaniu kwalifikowalnego podpisu elektronicznego i dostarczony do Zamawiającego w formie elektronicznej.
Audyt KRI oraz wdrożenie SZBI dla Zamawiającego muszą zostać przeprowadzone przez firmę która posiada własne zasoby w postaci:
1) audytora zewnętrznego (wiodącego) posiadającego przynajmniej jeden z certyfikatów określonych w rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu (Dz.U. 2018 poz. 1999) lub;
2) audytora wewnętrznego posiadającego przynajmniej jeden z certyfikatów określonych w rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu (Dz.U. 2018 poz. 1999) lub będącego audytorem wewnętrznym systemu zarządzania bezpieczeństwem informacji według normy PN-EN ISO/IEC 27001:2023.
3) a firma musi posiadać ISO 27001 wdrożone na cała organizację, a nie dla jakiegoś jednego procesu w firmie od minimum 5 lat i mieć praktyczne doświadczenie w zarządzaniu tego typu dokumentacją
Wykonawca przy świadczeniu usług jest zobowiązany uwzględnić i zastosować wymagania Dyrektywy Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) oraz akty wykonawcze wydane do niej. W przypadku jeżeli w okresie realizacji zamówienia zostanie przyjęta ustawa o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw bądź inne przepisy implementujące Dyrektywę Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) w polski system prawny Wykonawca ma obowiązek uwzględnić

wszystkie ich wymagania przy świadczeniu usług objętych niniejszym zamówieniem zarówno w trakcie realizacji zamówienia jak i w trakcie okresu gwarancji.
Celem usługi w ramach działania będzie wdrożenie procedur systemu zarządzania bezpieczeństwem informacji wdrożonych u Zamawiającego z uwzględnieniem uwarunkowań i specyfiki projektu oraz specyfiki jednostek. Analiza zostanie przeprowadzona zgodnie z wymogami ISO/IEC 27001:2023. W efekcie zostanie zaktualizowana także polityka bezpieczeństwa w zakresie ochrony danych osobowych. Usługa obejmuje również aktualizację dokumentów opisujących zbiory danych i ich zgodność z wymogami prawnymi oraz aktualizację dokumentów opisujących miejsca i sposoby przetwarzania danych osobowych.
Na usługę aktualizacji, opracowania i wdrożenia Systemu Zarządzania Bezpieczeństwem Informacji składają się co najmniej:
1. Wykonanie oceny obecnej dostępnej dokumentacji.
2. Określenie stanu faktycznego zabezpieczeń danych w systemach informatycznych poprzez przeprowadzenie audytu zabezpieczeń dostępu do danych oraz przygotowanie raportu wraz z zaleceniami i projektem zmian spełnienie wymagań normy PN-EN ISO/IEC 27001:2023 i zaleceń norm pokrewnych, oraz wymagań prawnych nałożonych na organizację, między innymi dotyczących ochrony danych osobowych.
3. Przeprowadzenie instruktażu wprowadzającego dla pracowników w zakresie ochrony informacji, inwentaryzacji aktywów informacyjnych oraz oceny ryzyka.
4. Aktualizacja/opracowanie Polityki Bezpieczeństwa zgodnej z wymaganiami normy PN-EN ISO/IEC 27001:2023 i zaleceń norm pokrewnych, oraz wymagań prawnych nałożonych na organizację, między innymi dotyczących ochrony danych osobowych w zakresie:
1) organizacja systemu bezpieczeństwa informacji;
2) zarządzanie aktywami;
3) zarządzanie zasobami ludzkimi;
4) organizacja bezpieczeństwa fizycznego i środowiskowego;
5) kontrola dostępu, zarządzania hasłami, stosowania zabezpieczeń kryptograficznych, czystego biurka i czystego ekranu, usuwania i niszczenia informacji, pracy w strefach bezpieczeństwa;
6) akwizycja, rozwój i utrzymanie systemu;
7) zarządzanie incydentami związanymi z bezpieczeństwem informacji;
8) zarządzanie ciągłością działania;
9) zarządzania kopiami zapasowymi;
10) zarządzania monitoringiem;
11) zoboiązanie do zachowania poufności, stosowania polityk i procedur SZBI;
12) używania urządzeń komputerowych;
13) metoda szacowania i postępowania z ryzykiem;
14) deklaracja stosowania
5. Wdrożenie Polityki Bezpieczeństwa Informacji. Poprzez wdrożenie należy rozumieć także aktualizację/utworzenie odpowiednich dokumentów po konsultacjach z pracownikami Zamawiającego, zatwierdzenie dokumentacji przez Kierownictwo Zamawiającego oraz przeprowadzenie instruktażu pracowników w zakresie wykonywania obowiązków zgodnie z opracowanym sposobem postępowania w dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji.
Ponad to:
1. W ramach realizacji zamówienia Wykonawca przy współpracy z Zamawiającym opracuje/zaktualizuje procedury bezpieczeństwa fizycznego obejmujące obowiązek wyznaczania osoby odpowiedzialnej za bezpieczeństwo fizyczne.
2. W ramach realizacji zamówienia Wykonawca przy współpracy z Zamawiającym opracuje/zaktualizuje zasady odpowiedzialności za cyberbezpieczeństwo wraz ze wskazaniem obowiązku wyznaczania osoby odpowiedzialnej za cyberbezpieczeństwo.

3. W ramach realizacji zamówienia Wykonawca przy współpracy z Zamawiającym opracuje/zaktualizuje politykę szkoleń z zakresu cyberbezpieczeństwa wraz z wprowadzeniem obowiązku regularnego, corocznego prowadzenia szkoleń.
4. W ramach realizacji zamówienia Wykonawca przy współpracy z Zamawiającym opracuje/zaktualizuje treść zarządzenia wdrażającego SZBI dla Zamawiającego.
5. W ramach realizacji zamówienia Wykonawca przy współpracy z Zamawiającym opracuje/zaktualizuje plan postępowania z ryzkiem obejmujący systematyczne tworzenie raportów oceny ryzyka w Jednostce oraz konieczność cyklicznego przeglądu tego raportu przez Kierownika JST.
6. W ramach realizacji zamówienia Wykonawca przy współpracy z Zamawiającym opracuje/zaktualizuje szczegółowy sposób realizacji celów oraz we współpracy z Zamawiającym przypisze odpowiedzialności za ich realizację.
7. W ramach realizacji zamówienia Wykonawca przy współpracy z Zamawiającym opracuje/zaktualizuje procedurę wprowadzającą obowiązek regularnego, corocznego przeglądu PBI jednostki.
8. W ramach realizacji zamówienia Wykonawca przy współpracy z Zamawiającym opracuje/zaktualizuje politykę szkoleń obejmującą obowiązek informowania o zmianach w PBI w toku okresowych szkoleń stanowiskowych.
9. W ramach realizacji zamówienia Wykonawca przy współpracy z Zamawiającym opracuje/zaktualizuje kluczowe aktywa informacyjne Jednostki (zbiory danych/ systemy/ usługi).
10. W ramach realizacji zamówienia Wykonawca przy współpracy z Zamawiającym opracuje/zaktualizuje rejestr ryzyk uwzględniający aktywa Jednostki.
11. W ramach realizacji zamówienia Wykonawca przy współpracy z Zamawiającym opracuje/zaktualizuje zagrożenia związane z cyberbezpieczeństwem w ramach procesów zarządczych oraz zarządzania ryzykiem.
12. W ramach realizacji zamówienia Wykonawca przy współpracy z Zamawiającym opracuje/zaktualizuje plan postępowania z ryzkiem związanym z zagrożeniami bezpieczeństwa informacji.
13. W ramach realizacji zamówienia Wykonawca przy współpracy z Zamawiającym opracuje/zaktualizuje kompleksową politykę zarządzania ryzykiem uwzględniającą obowiązek używania do określenia w Jednostce zagrożeń, podatności, prawdopodobieństwa ich wystąpienia i skutków.
14. W ramach realizacji zamówienia Wykonawca przy współpracy z Zamawiającym opracuje/zaktualizuje kompleksową politykę zarządzania ryzykiem uwzględniającą obowiązek identyfikacji i priorytetyzacji odpowiedzi na ryzyka.
15. W ramach realizacji zamówienia Wykonawca przy współpracy z Zamawiającym opracuje/zaktualizuje kompleksową politykę zarządzania ryzykiem uwzględniającą system oceny ryzyka.
16. W ramach realizacji zamówienia Wykonawca przy współpracy z Zamawiającym opracuje/zaktualizuje kompleksową politykę zarządzania ryzykiem cyberbezpieczeństwa uwzględniającą identyfikowane, ustanawiane i oceniane ryzyka.
17. W ramach realizacji zamówienia Wykonawca przy współpracy z Zamawiającym opracuje/zaktualizuje kompleksową politykę zarządzania danymi uwzględniającą polityki ich niszczenia, plan backup, plany reagowania i odtwarzania danych.
18. W ramach realizacji zamówienia Wykonawca przy współpracy z Zamawiającym opracuje/zaktualizuje plan zarządzania podatnościami.
19. W ramach realizacji zamówienia Wykonawca przy współpracy z Zamawiającym opracuje/zaktualizuje kompleksową politykę zarządzania zapisami zdarzeń / logów/ inspekcji.
20. W ramach realizacji zamówienia Wykonawca przy współpracy z Zamawiającym opracuje/zaktualizuje politykę użytkowania dostępu do odczytu lub zapisu danych z zewnętrznych nośników danych.

21. W ramach realizacji zamówienia Wykonawca przy współpracy z Zamawiającym opracuje/zaktualizuje kompleksową politykę reagowania na incydenty uwzględniającą procedury procesowania incydentów.
22. W ramach realizacji zamówienia Wykonawca przy współpracy z Zamawiającym opracuje/zaktualizuje plan zarządzania podatnościami uwzględniający obowiązek dokumentowania ryzyka z nimi związanego.
23. W ramach realizacji zamówienia Wykonawca przy współpracy z Zamawiającym opracuje/zaktualizuje politykę reagowania na incydenty uwzględniającą procedury procesowania incydentów i ich aktualizacji w obszarze doświadczeń i wniosków z wykrytych i obsłużonych incydentów.
24. W ramach realizacji zamówienia Wykonawca przy współpracy z Zamawiającym opracuje/zaktualizuje politykę reagowania na incydenty uwzględniającą procedury procesowania incydentów wraz z obowiązkiem ich aktualizacji.
25. W ramach realizacji zamówienia Wykonawca przy współpracy z Zamawiającym opracuje/zaktualizuje politykę planów odtwarzania uwzględniającą obowiązek ich aktualizacji w obszarze doświadczeń i wniosków z prowadzonych procesów odtwarzania.
Poszczególne etapy realizacji usługi.
Etap I. Audyt zerowy.
1. Określenie stanu spełnienia wymagań prawnych nałożonych na organizację w zakresie ochrony informacji.
2. Sprawdzenie spełnienia wymagań i zaleceń w ramach standardów PN-EN ISO/IEC 27001:2023 i norm pokrewnych.
3. Inwentaryzacja aktywów informacyjnych i ocena ryzyka.
4. Ocena zabezpieczeń technicznych, organizacyjnych oraz fizycznych.
5. Analiza dokumentacji Polityki Bezpieczeństwa Informacji.
6. Analiza dokumentacji Polityki Bezpieczeństwa Danych Osobowych.
7. Zestaw działań mających na celu określenie stanu faktycznego zabezpieczeń technicznych w systemie informatycznym:
1) Ocena schematu sieci.
2) Określenie rodzaju połączeń.
3) Określenie segmentów sieci.
4) Przeprowadzenie oceny środowiska informatycznego.
5) Ocena sposobu identyfikowania i logowania użytkowników.
6) Analiza zarządzania kontami użytkowników.
7) Analiza strony www pod kątem ochrony danych osobowych.
8) Analiza systemu backupów i archiwizacji danych.
9) Określenie miejsc redundancji w sieci i systemach informatycznych.
10) Analiza konfiguracji zabezpieczeń systemów operacyjnych na serwerach.
11) Analiza konfiguracji zabezpieczeń baz danych.
12) Określenie bezpieczeństwa aplikacji i serwerów WWW.
13) Analiza konfiguracji urządzeń sieciowych: switche, routery, IDS, IPS, UTM, firewall.
14) Ocena zabezpieczeń dostępu do sieci publicznej.
15) Analiza zabezpieczeń stacji roboczych.
16) Analiza ochrony danych na komputerach przenośnych.
17) Badanie zabezpieczeń nośników zewnętrznych.
18) Sprawdzenie procedur zarządzania ciągłością działania.
Etap II. Zastosowanie zabezpieczeń na podstawie zaleceń poaudytowych.
1. Konsultacje przy wdrożeniu zabezpieczeń w infrastrukturze systemu informatycznego;
2. Konsultacje przy wdrożeniu zabezpieczeń organizacyjnych - polityki bezpieczeństwa danych osobowych, zapisów w umowach z dostawcami itp.

Etap III. Planowanie Systemu Zarządzania Bezpieczeństwem Informacji (SZBI).
1. Przeprowadzenie instruktażu dla kadry zarządzającej z zasad bezpieczeństwa informacji.
2. Zakres SZBI:
1) określenie rodzaju działalności organizacji, jej lokalizacji, rodzajów aktywów i wykorzystywanych technologii;
2) określenie zasięgu organizacji;
3) badanie środowiska zewnętrznego, powiązań z innymi organizacjami, systemami oraz dostawcami.
3. Zdefiniowanie wymaganych polityk SZBI:
1) uwzględnienie rodzaju działalności organizacji, jej lokalizacji, rodzajów aktywów i wykorzystywanych technologii;
2) analiza wymagań prawnych oraz wymagań wynikających z umów;
3) uwzględnienie sposobu ustalania celów oraz wyznaczania kierunków działań w ramach systemu.
4. Szacowanie ryzyka:
1) wybór metody szacowania ryzyka;
2) określenie kryteriów akceptowalności ryzyk i identyfikacji akceptowalnych poziomów ryzyk;
3) zdefiniowanie obszarów zabezpieczeń objętych analizą ryzyka.
5. Wybór celów zabezpieczeń:
1) zdefiniowanie celów zabezpieczeń na podstawie listy zawartej w załączniku A normy PN-EN ISO/IEC 27001:2023;
2) zdefiniowanie własnych celów zabezpieczania i zabezpieczeń;
3) uwzględnienie wyników procesu szacowania ryzyka i określenie postępowania z ryzykiem;
4) określenie środków ochrony.
Etap IV. Inwentaryzacja i szacowanie ryzyka SZBI.
1. Przeprowadzenie instruktaży dla pracowników oraz kadry zarządzającej z metody inwentaryzacji i klasyfikacji aktywów informacyjnych.
2. Wykonanie wraz z pracownikami inwentaryzacji i klasyfikacji aktywów informacyjnych.
3. Zdefiniowanie planu postępowania z ryzykiem:
1) przeprowadzenie instruktaży dla kadry zarządzającej z wybranej metody oceny ryzyka;
2) szacowanie i ocena ryzyka - zaktualizowanie wartości ryzyka wynikające z audytu zerowego;
3) zdefiniowanie planu postępowania z ryzykiem;
4) określenie planu zarządzania zidentyfikowanymi i oszacowanymi ryzykami;
5) określenie zadań do realizacji, zdefiniowanie odpowiedzialności i ram czasowych.
4. Opracowanie raportu z oceny ryzyka.
Etap V. Opracowanie niezbędnej dokumentacji SZBI.
1. Opracowanie wspólnie z pracownikami Zamawiającego wymaganych procedur i instrukcji:
1) opracowanie przy współpracy z Zamawiającym Polityki Bezpieczeństwa Informacji;
2) opracowanie przy współpracy z Zamawiającym Instrukcji Zarządzania Systemem Informatycznym;
3) opracowanie przy współpracy z Zamawiającym procedur i instrukcji wymaganych przez normę PN-EN ISO/IEC 27001:2023;
4) opracowanie przy współpracy z Zamawiającym procedur i instrukcji dopasowanych do specyfiki działalności organizacji;
5) opracowanie przy współpracy z Zamawiającym Instrukcji postępowania na wypadek wykrycia incydentu naruszenia bezpieczeństwa;
6) opracowanie przy współpracy z Zamawiającym przy współpracy z Zamawiającym procedury audytu wewnętrznego;
7) opracowanie przy współpracy z Zamawiającym procedury nadzoru nad dokumentacją;
8) opracowanie przy współpracy z Zamawiającym procedury działań korygujących i zapobiegawczych;
9) opracowanie przy współpracy z Zamawiającym procedury zachowania ciągłości działania;

10) opracowanie przy współpracy z Zamawiającym wraz z pracownikami Zamawiającego planów ciągłości działania.
2. Wykonanie projektu zabezpieczeń - opracowanie projektu zabezpieczeń i konsultacje przy wdrożeniu odpowiednio skutecznych zabezpieczeń zgodnych z celami zabezpieczeń.
3. Opracowanie programu uświadamiania i szkolenia.
4. Przeprowadzenie instruktaży dla pracowników z dokumentacji ochrony informacji.
5. Przeprowadzenie instruktaży dla kadry zarządzającej z dokumentacji ochrony informacji.

Odp.
Zamawiający akceptuje proponowane rozwiązanie. W związku z powyższym, celem umożliwienia zapoznania się z powyższym, wszystkim potencjalnym wykonawcom, Zamawiający przedłuża termin przesłania odpowiedzi na rozeznanie cenowe do 07.03.2025 r. godz. 15.00

Dokument podpisany przez Krzysztof Petrykiewicz
Data: 2025.03.03 09:51:08 CET