Zespół Zakładów Opieki Zdrowotnej w Wadowicach
ul. Karmelicka 5, 34-100 Wadowice
www.zzozwadowice.pl, email: sekretariat@zzozwadowice.pl

Załącznik nr 1

Opis przedmiotu zamówienia

Przedmiotem zamówienia jest przeprowadzenie audytu spełnienia wymagań ustawy o krajowym systemie cyberbezpieczeństwa przez operatora usługi kluczowej (Zamawiającego) zgodnie z wymogami Ustawy o krajowym systemie cyberbezpieczeństwa, aktów powiązanych oraz szablonem sprawozdania z audytu zgodnego z ustawą o Krajowym Systemie Cyberbezpieczeństwa rekomendowanym przez Ministerstwo Cyfryzacji.

Warunki i zakres przeprowadzenia audytu końcowego w zakresie sprawdzenia bezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej z wymaganiami Ustawy:
a) Analiza procesów przetwarzania danych wraz z analizą stanu zabezpieczeń systemowych.
b) Identyfikacja informacji i jej klasyfikacja.
c) Inwentaryzacja zasobów infrastruktury teleinformatycznej, oprogramowania i obszarów bezpiecznych,
d) Identyfikacja i analiza podatności systemów wspomagających świadczenie usługi kluczowej.

Wynikiem analizy musi być pełna lista przeskanowanych pod kątem podatności, systemów zawierająca informacje obejmujące: skanowany system operacyjny, uruchomione na nim usługi, otwarte porty komunikacyjne, listę wykrytych podatności oraz wytyczne dotyczące sposobu usunięcia wykrytych podatności. W celu wykonania powyższych czynności, Wykonawca zobowiązany jest do zapewnienia odpowiedniej licencji na system skanujący.
e) Analiza bezpieczeństwa fizycznego i środowiskowego dla zabezpieczenia realizacji usługi kluczowej.
f) Zarządzanie: ryzykiem, incydentem, podatnościami, środkami technicznymi i organizacyjnymi, systemem monitorowania w trybie ciągłym.
g) Inwentaryzacja procedur.
h) Bezpieczeństwo i ciągłość dostaw i usług od których zależy świadczenie usługi kluczowej.
i) Przegląd dokumentacji związanej z cyberbezpieczeństwem.
j) Zidentyfikowaniu wszelkich niezgodności i wdrożenie działań naprawczych.

Audyt będzie się opierać na wizji lokalnej przeprowadzonej przez wskazane przez Wykonawcę osoby w wybranych lokalizacjach Zamawiającego oraz z wykorzystaniem zdalnego dostępu. Ponadto analiza oparta będzie o wywiad i oświadczenia wskazanych przez Zamawiającego osób.

Audyt bezpieczeństwa, może być przeprowadzony przez:
·jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016r. o systemach oceny zgodności i nadzoru rynku (t.j. Dz. U. z 2022 r. poz. 5 z późn. zm.), w zakresie właściwym do podejmowanych ocen bezpieczeństwa systemów informacyjnych;
·co najmniej dwóch audytorów posiadających:
- certyfikaty określone w poniższym wykazie certyfikatów uprawiających do przeprowadzenia audytu lub

- co najmniej trzyletnią praktykę w zakresie audytu bezpieczeństwa systemów informacyjnych, lub
- co najmniej dwuletnią praktykę w zakresie audytu bezpieczeństwa systemów informacyjnych i legitymujących się dyplomem ukończenia studiów podyplomowych w zakresie audytu bezpieczeństwa systemów informacyjnych, wydanym przez jednostkę organizacyjną, która w dniu wydania dyplomu była uprawniona, zgodnie z odrębnymi przepisami, do nadawania stopnia naukowego doktora nauk ekonomicznych, technicznych lub prawnych;

Wykaz certyfikatów uprawniających do przeprowadzenia audytu:
• Certified Internal Auditor (CIA);
• Certified Information System Auditor (CISA);
• Certyfikat audytora wiodącego systemu zarządzania bezpieczeństwem informacji według normy PN- EN ISO/IEC 27001 wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku, w zakresie certyfikacji osób;
• Certyfikat audytora wiodącego systemu zarządzania ciągłością działania PN-EN ISO 22301 wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku, w zakresie certyfikacji osób;
• Certified Information Security Manager (CISM);
• Certified in Risk and Information Systems Control (CRISC);
• Certified in the Governance of Enterprise IT (CGEIT);
• Certified Information Systems Security Professional (CISSP);
• Systems Security Certified Practitioner (SSCP);
• Certified Reliability Professional;
• Certyfikaty uprawniające do posiadania tytułu ISA/IEC 62443 Cybersecurity Expert.

W celu potwierdzenia spełnienia powyższych wymagań Wykonawca zobowiązany jest do przedłożenia wraz z ofertą w/w certyfikatów.

Wnioski wypływające z audytu powinny wskazywać na potrzebę podjęcia działań korygujących, naprawczych lub doskonalących, jeżeli ma to zastosowanie. Wynikiem audytu będzie sporządzenie przez Wykonawcę raportu, w formie papierowej oraz elektronicznej, określającego konieczne działania, a także zawierającego specyfikację rozwiązań sprzętowych oraz programowych wraz z kompleksową informacją na temat ich wdrożenia i wykorzystania u Zamawiającego celem osiągnięcia zgodności z wymaganiami Ustawy.

Powyższe wytyczne, rekomendacje oraz opisy techniczne rozwiązań (wraz z szacunkową wyceną) dotyczące sposobu wdrożenia odpowiednich, do oszacowanego ryzyka, środków technicznych i organizacyjnych, po winny obejmować m.in.:
• utrzymania i bezpiecznej eksploatacji systemu informacyjnego,
• bezpieczeństwa fizycznego i środowiskowego, uwzględniając kontrolę dostępu,
• bezpieczeństwa oraz ciągłości dostaw i usług, od których zależy świadczenie usługi kluczowej,
• wdrażania, dokumentowania i utrzymywania planów działania umożliwiających ciągłe i niezakłócone świadczenie usługi kluczowej oraz zapewniających poufność, integralność, dostępność i autentyczność informacji,
• objęcia systemu informacyjnego, wykorzystywanego do świadczenia usługi kluczowej, systemem monitorowania w trybie ciągłym,
• wdrożenia odpowiednich środków organizacyjnych wymaganych ustawą w celu świadczenia usługi kluczowej,
• wdrożenia wymaganej ustawą dokumentacji systemu cyberbezpieczeństwa.

Obszary Audytu:

a) Ocena skuteczności działania infrastruktury w zakresie urządzeń i konfiguracji w zakresie: ochrony poczty, ochrony sieci, systemów serwerowych, stacji roboczych, systemów bezpieczeństwa,

b) Zarządzanie bezpieczeństwem informacji:

- nośniki wymienne - udokumentowany sposób postępowania,
- zarządzanie tożsamością/dostęp do systemów w zakresie: przydzielanie dostępu, odbieranie dostępu,
- pomieszczenie/pomieszczenia w dyspozycji struktur zespołu odpowiedzialnego za cyberbezpieczeństwozgodnie z wymogami dla Operatora Usługi Kluczowej, o którym mowa w art. 5 ustawy z dnia 5 lipca 2018 r. o Krajowym Systemie Cyberbezpieczeństwa.

c) Monitorowanie i reagowanie na incydenty bezpieczeństwa:

- procedury zarządzania incydentami,
- raportowanie poziomów pokrycia scenariuszami znanych incydentów,
- dokumentacja dotycząca przekazywania informacji do właściwego zespołu CSIRT poziomu krajowego/ sektorowego zespołu cyberbezpieczeństwa,
- monitorowanie i wykrycie incydentów bezpieczeństwa,
- Identyfikacja i dokumentowanie przyczyn wystąpienia incydentów.

d) Zarządzanie ciągłością działania:

- konfiguracja oraz polityki systemów do wykonywania kopii bezpieczeństwa,
- raport z przeglądów i testów odtwarzania kopii bezpieczeństwa,
- procedury wykonywania i przechowywania kopii zapasowych,
- strategia i polityka ciągłości działania, awaryjne oraz odtwarzania po katastrofie (DRP),
- procedury utrzymaniowe.

e) Utrzymanie systemów informacyjnych:

- harmonogramy skanowania podatności,
- aktualny status realizacji postępowania z podatnościami,
- procedury związane ze z identyfikowaniem (wykryciem) podatności,
- współpraca z osobami odpowiedzialnymi za procesy zarządzania incydentami.

f) Zarządzanie bezpieczeństwem i ciągłością działania łańcucha usług:

- polityka bezpieczeństwa w relacjach z dostawcami,
- standardy i wymagania nakładane na dostawców w umowach w zakresie cyberbezpieczeństwa,
- dostęp zdalny,

<u>Niespełnienie jakiegokolwiek parametru będzie skutkowało odrzuceniem oferty</u>.