Załącznik nr 1 do Zapytania Ofertowego

OPIS PRZEDMIOTU ZAMÓWIENIA

I. Cel audytu

Przedmiotem postępowania jest przeprowadzenie audytu na podstawie „ZARZĄDZENIA NR 68/2022/BBIICD PREZESA NARODOWAEGO FUNDUSZU ZDROWIA z dnia 20 maja 2022 r. w sprawie finasowania działań w celu podniesienia poziomu bezpieczeństwa systemów teleinformatycznych świadczeniodawców."

Celem audytu jest wykazanie przez świadczeniodawcę (tu: Zamawiającego) podniesienia poziomu bezpieczeństwa teleinformatycznego po zrealizowaniu określonych czynności, zgodnie z ww. Zarządzeniem (Załącznik nr 3 do Zapytania Ofertowego) w odniesieniu do stanu na dzień przeprowadzania badania dojrzałości cyberbezpieczeństwa w przedsiębiorstwie Zamawiającego.

II. Sposób realizacji prac

1. Audyt związany będzie z przeprowadzeniem wizji lokalnej przez wskazane przez Wykonującego osoby w lokalizacji Zamawiającego. Jednocześnie analiza oparta będzie o wywiad i informacje od osób wskazanych przez Zamawiającego.
2. Audyt zostanie przeprowadzony w 3 warstwach: metodologicznej, dokumentacyjnej, organizacyjnej.
3. Przedmiotowa analiza i ocena cyberbezpieczeństwa musi być realizowana w oparciu o obowiązującą normę PN ISO/IEC 27001.

III. Wymagania dotyczące audytu bezpieczeństwa

1. Wykonawca zobowiązuje się do:
   1) Przeprowadzenia audytu początkowego, mającego na celu zapoznanie się z obecną sytuacją dot. poziomu bezpieczeństwa teleinformatycznego w przedsiębiorstwie Zamawiającego, z uwzględnieniem oceny ankietowej placówki wynikającej z „ZARZĄDZENIA NR 68/2022/BBIICD PREZESA NARODOWAEGO FUNDUSZU ZDROWIA z dnia 20 maja 2022 r. w sprawie finasowania działań w celu podniesienia poziomu bezpieczeństwa systemów teleinformatycznych świadczeniodawców". Analiza powinna przede wszystkim dotyczyć czynności objętych finansowaniem, tj. działań zawartych w *Rozdziale 2. Warunki udzielania finansowania* ww. zarządzenia. Audyt nastąpi w ciągu 1 tygodnia od dnia podpisania umowy.
   2) Opracowania analizy aktualnego stanu poziomu bezpieczeństwa teleinformatycznego z uwzględnieniem wyników audytu początkowego wraz ze wskazaniem zagadnień wymagających usprawnienia.
   3) Przeprowadzenia audytu końcowego, wykonanego po zrealizowaniu wszystkich zakupów zaplanowanych w projekcie. Audyt będzie miał na celu dokonanie oceny poziomu bezpieczeństwa teleinformatycznego, po wdrożeniu w przedsiębiorstwie Zamawiającego szeregu czynności zapewniających zwiększenie owego poziomu bezpieczeństwa systemów teleinformatycznych, wykorzystywanych do udzielania świadczeń opieki zdrowotnej. Audyt nastąpi w ciągu 2 tygodni od powiadomienia przez Zamawiającego o zakończeniu procesu realizacji zakupów i wdrażania zakupionych usług czy oprogramowania.

4) Opracowania wyników dotyczących poziomu bezpieczeństwa teleinformatycznego przed oraz po wdrożeniu czynności mających na celu zwiększenie owego poziomu, z uwzględnieniem rekomendacji odnośnie zasadności realizacji tego projektu. Wyniki powinny być przedstawione w ciągu 1 tygodnia od zakończenia audytu końcowego.

2. Audyt bezpieczeństwa – zgodnie z „ZARZĄDZENIEM NR 68/2022/BBIICD PREZESA NARODOWAEGO FUNDUSZU ZDROWIA z dnia 20 maja 2022 r. w sprawie finasowania działań w celu podniesienia poziomu bezpieczeństwa systemów teleinformatycznych świadczeniodawców", może być przeprowadzony przez:
   1) jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku (Dz. U. z 2022 r. poz. 5), w zakresie właściwym do podejmowanych ocen bezpieczeństwa systemów informacyjnych;
   2) co najmniej dwóch audytorów posiadających:
      a) certyfikaty określone w poniższym wykazie certyfikatów uprawiających do przeprowadzenia audytu lub
      b) co najmniej trzyletnią praktykę w zakresie audytu bezpieczeństwa systemów informacyjnych, lub
      c) 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:

   1. Certified Internal Auditor (CIA);
   1) Certified Information System Auditor (CISA);
   2) 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*;
   3) 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*;
   4) Certified Information Security Manager (CISM);
   5) Certified in Risk and Information Systems Control (CRISC);
   6) Certified in the Governance of Enterprise IT (CGEIT);
   7) Certified Information Systems Security Professional (CISSP);
   8) Systems Security Certified Practitioner (SSCP);
   9) Certified Reliability Professional;
   10) Certyfikaty uprawniające do posiadania tytułu ISA/IEC 62443 Cybersecurity Expert.

Załącznik nr 1 do Zapytania Ofertowego

Weryfikacja bezpieczeństwa ma obejmować następujące obszary:

Nazwa obszaru	**Opis działań skutkujących podniesieniem poziomu bezpieczeństwa teleinformatycznego świadczeniodawców**
Skuteczność działania infrastruktury	– Urządzenia i konfiguracja w zakresie ochrony poczty – Urządzenia i konfiguracja w zakresie ochrony sieci – Urządzenia i konfiguracja w zakresie systemów serwerowych – Urządzenia i konfiguracja w zakresie stacji roboczych – Urządzenia i konfiguracja w zakresie systemów bezpieczeństwa
Procesy zarządzania bezpieczeństwem informacji	– Nośniki wymienne – udokumentowany sposób postępowania – Zarządzanie tożsamością / dostęp do systemów w zakresie: -- Przydzielanie dostępu -- Odbieranie dostępu – Pomieszczenie w dyspozycji struktur zespołu odpowiedzialnego za cyberbezpieczeństwo w przypadku podmiotów, które otrzymały decyzję uznającą taki podmiot za operatora usługi kluczowej, o którym mowa w art. 5 *ustawy z dnia 5 lipca 2018 r. o Krajowym Systemie Cyberbezpieczeństwa*
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
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
Utrzymanie systemów informacyjnych	– Harmonogramy skanowania podatności – Aktualny status realizacji postępowania z podatnościami – Procedury związane z identyfikowaniem (wykryciem) podatności – Współpraca z osobami odpowiedzialnymi za procesy zarządzania incydentami
Zarządzanie bezpieczeństwem i ciągłością działania łańcucha dostaw	– Polityka bezpieczeństwa w relacjach z dostawcami – Standardy i wymagania nakładane na dostawców w umowach w zakresie cyberbezpieczeństwa – Dostęp zdalny – Metody uwierzytelniania

IV. Oczekiwany produkt finalny

Produkt finalny ma stanowić ocena systemu bezpieczeństwa cybernetycznego Zamawiającego zgodnie z ustawą, obejmującą:

1) Opracowanie raportu przeprowadzonej analizy zgodnie z metodyką ISO 27001, w tym:
   a. Określenie niezgodności;
   b. Dla zgodności określenie potencjału do doskonalenia i opracowanie rekomendacji odnośnie wdrożenia adekwatnych zabezpieczeń technicznych i organizacyjnych.
2) Wytyczne, rekomendacje oraz opisy techniczne rozwiązań wraz z szacunkową wyceną, dotyczące sposobu wdrożenia odpowiednich środków technicznych i organizacyjnych, w tym utrzymania i bezpiecznej eksploatacji systemu informacyjnego.

Przeprowadzony audyt musi wykazać podniesienie poziomu bezpieczeństwa teleinformatycznego w odniesieniu do poziomu wynikającego z ankiety lub jego brak. Raport musi zawierać jasne stanowisko audytora w zakresie wykazania, że spożytkowane środki wpłynęły na podniesienie poziomu bezpieczeństwa w przedsiębiorstwie Zamawiającego.