

## Załącznik nr 1 – opis wymagań do zapytania ofertowego

**Przedmiotem zamówienia jest przeprowadzenie audytu, będącego konsekwencją zakupu i wdrożenia platformy środowiska pracy awaryjnej oraz centrum kopii zapasowej, którego wynik potwierdzi utworzenie odmiejscowionej kopii zapasowej i odtworzenie z niej kompletnego systemu oraz wykonanej dokumentacji bezpieczeństwa.**

Celem audytu jest wykazanie podniesienia poziomu bezpieczeństwa teleinformatycznego po zrealizowaniu czynności w odniesieniu do stanu na dzień przeprowadzenia badania poziomu dojrzałości cyberbezpieczeństwa u świadczeniodawcy w formie „Ankiety weryfikacji dojrzałości pod kątem bezpieczeństwa”.

Przeprowadzony audyt powinien wykazać podniesienie poziomu bezpieczeństwa teleinformatycznego w odniesieniu do poziomu wynikającego z ankiety lub jego brak.

Raport musi zawierać jasne stanowisko audytora w zakresie wykazania, czy spożytkowane środki wpłynęły na podniesienie poziomu bezpieczeństwa w placówce.

### **Ramowy harmonogram wykonania usługi:**

1. Audyt początkowy – audyt mający na celu zapoznanie się ze stanem początkowym dot. poziomu bezpieczeństwa teleinformatycznego w placówce.

Głównym aspektem analizy powinny być elementy możliwe do finansowania opisane w załączniku Nr 1 do zarządzenia Nr 8/2023/BBIICD Prezesa Narodowego Funduszu Zdrowia z dnia 16 stycznia 2023 r.:

2. Opracowanie ramowej analizy stanu aktualnego dot. poziomu bezpieczeństwa teleinformatycznego z uwzględnieniem wyników audytu w pkt.1 wraz ze wskazaniem elementów do usprawnienia.

3. Audyt końcowy – wykonywany po realizacji wszystkich zakupów w projekcie. Audyt poziomu bezpieczeństwa teleinformatycznego w placówce uwzględniający elementy wdrożone w ramach realizacji aspektów wskazanych przez Zamawiającego podczas realizacji umowy z NFZ w ramach rzeczonoego zarządzenia.

4. Opracowanie wyników stanu pierwotnego i stanu po realizacji projektu wraz z uwzględnieniem rekomendacji dot. zasadności i kompletności realizacji projektu.

### **Wymagania dotyczące audytu bezpieczeństwa:**

na podstawie załącznika Nr 2 do zarządzenia Nr 8/2023/BBIICD Prezesa Narodowego Funduszu Zdrowia z dnia 16 stycznia 2023 r.:

1. Audyt bezpieczeństwa 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.

2. Wykaz certyfikatów uprawniających do przeprowadzenia audytu:

- 1) Certified Internal Auditor (CIA);
- 2) Certified Information System Auditor (CISA);
- 3) 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;

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

3. Celem audytu jest wykazanie przez Świadczeniodawcę podniesienia poziomu bezpieczeństwa teleinformatycznego po zrealizowaniu czynności zgodnie z niniejszym zarządzeniem oraz w obszarach wskazanych w poniższej tabeli w odniesieniu do stanu na dzień przeprowadzenia badania poziomu dojrzałości cyberbezpieczeństwa u Świadczeniodawcy w formie ankiety. Przeprowadzony audyt wykaże podniesienie poziomu bezpieczeństwa teleinformatycznego w odniesieniu do poziomu wynikającego z ankiety lub jego brak.

Nazwa obszaru	Opis działań skutkujących podniesieniem poziomu bezpieczeństwa teleinformatycznego u Świadczeniodawców.
Skuteczność działania infrastruktury.	<ul style="list-style-type: none"> <li>-Urządzenia i konfiguracja w zakresie ochrony poczty.</li> <li>-Urządzenia i konfiguracja w zakresie ochrony sieci.</li> <li>-Urządzenia i konfiguracja w zakresie systemów serwerowych.</li> <li>-Urządzenia i konfiguracja w zakresie stacji roboczych.</li> <li>-Urządzenia i konfiguracja w zakresie systemów bezpieczeństwa.</li> </ul>
Procesy zarządzania bezpieczeństwem informacji.	<ul style="list-style-type: none"> <li>-Nośniki wymienne - udokumentowany sposób postępowania.</li> <li>-Zarządzanie tożsamością/dostęp do systemów w zakresie:               <ul style="list-style-type: none"> <li>- - przydzielanie dostępu,</li> <li>- - odbieranie dostępu.</li> </ul> </li> <li>-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.</li> </ul>
Monitorowanie i reagowanie na incydenty bezpieczeństwa.	<ul style="list-style-type: none"> <li>-Procedury zarządzania incydentami.</li> <li>-Raportowanie poziomów pokrycia scenariuszami znanych incydentów.</li> <li>-Dokumentacja dotycząca przekazywania informacji do właściwego zespołu CSIRT poziomu krajowego/sektorowego zespołu cyberbezpieczeństwa.</li> <li>-Monitorowanie i wykrycie incydentów bezpieczeństwa.</li> <li>-Identyfikacja i dokumentowanie przyczyn wystąpienia incydentów.</li> </ul>
Zarządzanie ciągłością działania.	<ul style="list-style-type: none"> <li>-Konfiguracja oraz polityki systemów do wykonywania kopii bezpieczeństwa.</li> <li>-Raport z przeglądów i testów odtwarzania kopii bezpieczeństwa.</li> <li>-Procedury wykonywania i przechowywania kopii zapasowych.</li> <li>-Strategia i polityka ciągłości działania, awaryjne oraz odtwarzania po katastrofie (DRP).</li> <li>-Procedury utrzymaniowe.</li> </ul>
Utrzymanie systemów informacyjnych.	<ul style="list-style-type: none"> <li>-Harmonogramy skanowania podatności.</li> </ul>

	<ul style="list-style-type: none"> <li>-Aktualny status realizacji postępowania z podatnościami.</li> <li>-Procedury związane ze z identyfikowaniem (wykryciem) podatności.</li> <li>-Współpraca z osobami odpowiedzialnymi za procesy zarządzania incydentami.</li> </ul>
Zarządzanie bezpieczeństwem i ciągłością działania łańcucha usług	<ul style="list-style-type: none"> <li>-Polityka bezpieczeństwa w relacjach z dostawcami.</li> <li>-Standardy i wymagania nakładane na dostawców w umowach w zakresie cyberbezpieczeństwa.</li> <li>-Dostęp zdalny.</li> <li>-Metody uwierzytelnienia.</li> </ul>
Weryfikacja podniesienia poziomu bezpieczeństwa.	Przeprowadzony audyt wykazał podniesienie poziomu bezpieczeństwa teleinformatycznego w stosunku do stanu sprzed przystąpienia do działań mających na celu podniesienie poziomu bezpieczeństwa teleinformatycznego finansowanych w ramach zarządzenia.

Wymagany termin wykonania zamówienia do 23.10.2023r.