**Załącznik nr 5**

**OPIS PRZEDMIOTU ZAMÓWIENIA**

**Część I –**

**1a) Audyt Końcowy – 1 sztuka (zestaw)**

Wykonanie audytu bezpieczeństwa zgodnie z wymaganiami określonymi w kryteriach akceptacji do oceny przy audycie końcowym w obszarze cyberbezpieczeństwa w ramach inwestycji D.1.1.2 „Przyspieszenie procesów transformacji cyfrowej ochrony zdrowia poprzez dalszy rozwój usług cyfrowych w ochronie zdrowia”.

Celem audytu końcowego jest potwierdzenie spełnienia kryteriów akceptacji w obszarze cyberbezpieczeństwa określonych dla Inwestycji D.1.1.2, w tym uzyskanie co najmniej oceny pozytywnej lub warunkowo pozytywnej, zgodnie z Ankietą weryfikacji dojrzałości w zakresie cyberbezpieczeństwa, stanowiącą podstawę samooceny Zamawiającego na etapie składania wniosku o objęcie przedsięwzięcia wsparciem.

Wykonawca audytu zobowiązany jest do przedstawienia wyników audytu w formie tabelarycznej, zawierającej:

- odniesienie do każdego kryterium Ankiety weryfikacji dojrzałości w zakresie cyberbezpieczeństwa,

- wskazanie statusu: spełnione /niespełnione /spełnione warunkowo,

- krótkie, jednoznaczne uzasadnienie dokonanej oceny.

Audyt obejmuje wykonanie testów bezpieczeństwa o charakterze weryfikacyjnym, mających na celu potwierdzenie skuteczności wprowadzonych zabezpieczeń oraz zgodności konfiguracji systemów z dokumentacją powykonawczą, zgodnie z kryteriami akceptacji Inwestycji D.1.1.2.

Testy te nie mają charakteru testów penetracyjnych ani testów inwazyjnych i nie obejmują prób omijania zabezpieczeń, wykorzystywania podatności, symulacji ataków ani działań mogących powodować zakłócenia pracy systemów produkcyjnych, o ile Zamawiający nie zleci ich odrębnie.

W ramach realizacji audytu Wykonawca dostarczy:

- raport główny z audytu,

- mapowanie wyników audytu do kryteriów Ankiety weryfikacji dojrzałości,

- ocenę końcową audytu (pozytywna / warunkowo pozytywna),

- plan działań naprawczych lub doskonalących - jeżeli dotyczy,

- oświadczenie potwierdzające zgodność przeprowadzonego audytu z wymaganiami Inwestycji D.1.1.2.

Audyt powinien obejmować niezbędną infrastrukturę teleinformatyczną podmiotu, w tym przynajmniej bezpieczeństwo takich elementów jak:

• Kanały komunikacji jak np. poczta

• Sieciowe urządzenia brzegowe wraz z zasadami segmentacji oraz przepływów

• Kontrolery domeny

• Platforma wirtualizacyjna

• System zarządzania kopiami zapasowymi

• Poprawność konfiguracji stacji roboczych oraz serwerów

• Sposoby uwierzytelniania się użytkowników

Audyt realizowany będzie przez zespół audytujący składający się z co najmniej dwóch audytorów posiadających certyfikaty określone w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. ( Dz.U. poz. 1999) w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu lub co najmniej dwóch audytorów posiadających co najmniej trzyletnią praktykę w zakresie audytu bezpieczeństwa systemów informacyjnych lub jednostka oceniająca zgodność, akredytowana zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku (Dz. U. z 2022 r. poz. 1854 z późn.zm.), w zakresie właściwym do podejmowanych ocen bezpieczeństwa systemów informacyjnych.

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | **Opis parametru** | **Parametr wymagany** | **Parametr oferowany** |
|  | **System kopii zapasowych** |  |  |
|  | Kryteria akceptacji do oceny przy audycie końcowym w obszarze cyberbezpieczeństwa:  • Zestawienie wszystkich kluczowych i pomocniczych systemów objętych systemem kopii zapasowych – dla zakupu sprzętu i oprogramowania oraz usług wdrożeniowych.  • Dokument zawierający wymagania dotyczące częstotliwości wykonywania kopii zapasowych – dla zakupu sprzętu i oprogramowania oraz usług wdrożeniowych.  • Kompletna dokumentacja wdrożonego rozwiązania systemu kopii zapasowych w szczególności zestaw procedur wykonywania, odtworzenia (w tym cyklicznych testów), zabezpieczenia odmiejscowionej kopii, monitoringu i weryfikacji poprawności działania systemu, zarządzania uprawnieniami i dostępem do systemu – dla zakupu sprzętu i oprogramowania oraz usług wdrożeniowych.  • Raport z testów funkcjonalnych i niefunkcjonalnych działania systemu backupu – dla zakupu sprzętu i oprogramowania oraz usług wdrożeniowych.  • Potwierdzenie uczestnictwa na szkoleniach z zakresu obsługi systemu kopii zapasowej – w zakresie usług szkoleniowych.  • Wyniki testu potwierdzającego skuteczności wprowadzonych zabezpieczeń i potwierdzającego zgodność konfiguracji z dokumentacją – dla usług testów bezpieczeństwa.  • Wyciąg z umowy obejmujący zakres usługi – dla usług utrzymaniowych | Tak |  |
|  | **Zapory sieciowe** |  |  |
|  | Kryteria akceptacji do oceny przy audycie końcowym w obszarze cyberbezpieczeństwa:  • Dokumentacja powykonawcza wdrożonych zapór sieciowych wraz z zabezpieczeniami – dla zakupu sprzętu i oprogramowania oraz usług wdrożeniowych.  • Wyniki testu potwierdzającego skuteczność wprowadzonych zabezpieczeń i potwierdzającego zgodność konfiguracji z dokumentacją – dla usług testów bezpieczeństwa.  • Potwierdzenie uczestnictwa na szkoleniach z zakresu obsługi zainstalowanych zapór sieciowych – dla usług szkoleniowych.  • Wyciąg z umowy obejmujący zakres usługi – dla usług utrzymaniowych. | Tak |  |
|  | **Ochrona poczty e-mail** |  |  |
|  | Kryteria akceptacji do oceny przy audycie końcowym w obszarze cyberbezpieczeństwa:  • Opis sposobu ochrony poczty wraz z dokumentacją systemów ochrony poczty  • Protokół z testów, który opisuje wyniki testów wdrożonych polityk ochrony poczty w tym weryfikację mechanizmów (SPF, DMARC, DKIM) ochrony poczty elektronicznej przy pomocy portalu CERT Polska https://bezpiecznapoczta.cert.pl/  • Wynik testu potwierdzającego wdrożenie obowiązkowego drugiego składnika uwierzytelniającego (2FA) dla poczty elektronicznej dostępnej publicznie.  • Raport z wykonania backupu poczty elektronicznej wraz testowym odtworzeniem.  • Raport zawierający informacje o aktualizacji systemu pocztowego wraz z jego ochroną | Tak |  |
|  | **Segmentacja sieci** |  |  |
|  | Kryteria akceptacji do oceny przy audycie końcowym w obszarze cyberbezpieczeństwa:   * Dokument zawierający wymagania dotyczące podziału sieci wraz ze sposobem implementacji – dla zakupu sprzętu, oprogramowania oraz usług wdrożeniowych. * Dokumentacja sposobu identyfikowania, uwierzytelniania i autoryzacji urządzeń podłączanych do sieci – dla zakupu oprogramowania. * Wynik weryfikacji zgodności konfiguracji z dokumentacją– dla zakupu sprzętu, oprogramowania oraz usług wdrożeniowych. * Potwierdzenie uczestnictwa na szkoleniach z zakresu obsługi zainstalowanych systemów ochrony sieciowej – dla usług szkoleniowych * Wyciąg z umowy obejmujący zakres usługi – dla usług utrzymaniowych. * Wyniki testu potwierdzającego skuteczność wprowadzonych zabezpieczeń i potwierdzającego zgodność konfiguracji z dokumentacją – dla usług testów bezpieczeństwa. | Tak |  |
|  | **Ochrona stacji roboczych oraz serwerów (rozwiązania klasy EDR)** |  |  |
|  | Kryteria akceptacji do oceny przy audycie końcowym w obszarze cyberbezpieczeństwa:   * Dokumentacja powykonawcza wdrożonego rozwiązania, potwierdzająca zastosowanie polityk bezpieczeństwa oraz wdrożenie agentów rozwiązania na stacjach roboczych oraz serwerach – dla zakupu sprzętu i oprogramowania oraz usług wdrożeniowych. * Wyciąg z umowy obejmujący zakres usługi – dla usług utrzymaniowych. * Potwierdzenie uczestnictwa na szkoleniach z zakresu obsługi systemu – dla usług szkoleniowych. | Tak |  |
|  | **Zarządzanie podatnościami** |  |  |
|  | Kryteria akceptacji do oceny przy audycie końcowym w obszarze cyberbezpieczeństwa:   * Dokumentacja powykonawcza wdrożonego i uruchomionego systemu, wskazująca na obszary objęte skanowaniem podatności – dla zakupu oprogramowania lub zakupu wsparcia oraz usług wdrożeniowych. * Potwierdzenie uczestnictwa w szkoleniach – dla usług szkoleniowych. * Wyciąg z umowy obejmujący zakres usługi – dla usług utrzymaniowych. | Tak |  |
|  | **System zarządzania bezpieczeństwem informacji** |  |  |
|  | Kryteria akceptacji do oceny przy audycie końcowym w obszarze cyberbezpieczeństwa:   * Oświadczenie osoby uprawnionej do reprezentacji podmiotu, że kierownictwo ustanowiło lub zmodyfikowało System Zarządzania Bezpieczeństwem Informacji, oraz że zostały alokowane zasoby ludzkie i finansowe, niezbędne do jej realizacji, monitorowania i okresowych przeglądów. * Lista opracowanej dokumentacji wraz z opisem * Potwierdzenie uczestnictwa w szkoleniach – dla usług szkoleniowych | Tak |  |
|  | **Szkolenia z zakresu podnoszenia świadomości w obszarze cyberbezpieczeństwa (cyberhigieny)** |  |  |
|  | Kryteria akceptacji do oceny przy audycie końcowym w obszarze cyberbezpieczeństwa:   * Konspekt programu szkoleń   Potwierdzenie uczestnictwa w szkoleniach co najmniej 75% pracowników szpitala, pracujących na stacjach roboczych – oświadczenie dyrektora szpitala | Tak |  |
|  | **Usługi zarządzane bezpieczeństwa** |  |  |
|  | Kryteria akceptacji do oceny przy audycie końcowym w obszarze cyberbezpieczeństwa:   * Umowa o świadczenie usług Centrum Operacji Bezpieczeństwa – w zakresie usług SOC. * Wykaz przygotowanych Scenariuszy Reakcji dla zidentyfikowanych zagrożeń – w zakresie usługi przygotowania i wdrożenia scenariuszy. * Umowa o świadczenie usług udostępniania i zarządzania systemem SIEM – w zakresie tego systemu.   Umowa o świadczenie usług testów bezpieczeństwa – w zakresie usług testów. | Tak |  |
|  | **Uwierzytelnienie i autoryzacja do systemów** |  |  |
|  | * Dokumentacja powykonawcza wdrożonych rozwiązań uwierzytelniających wraz z zabezpieczeniami – dla zakupu urządzeń i oprogramowania oraz usług wdrożeniowych. * Potwierdzenie uczestnictwa w szkoleniach – dla usług szkoleniowych. | Tak |  |
|  | Termin wykonania audytu do 31.05.2026 | TAK |  |