

OPIS PRZEDMIOTU ZAMÓWIENIA

Audyt końcowy w obszarze cyberbezpieczeństwa

Specyfikacja parametrów funkcjonalno - technicznych

Przedmiotem zamówienia jest usługa audytu cyberbezpieczeństwa systemów informatycznych Szpitala w ramach projektu Rozwój usług cyfrowych w Samodzielnym Publicznym Zakładzie Opieki Zdrowotnej Wojewódzkim Szpitalu Specjalistycznym nr 3 w Rybniku w ramach KPO na lata 2021-2026 DZIAŁANIE 1.1.2 „Przyspieszenie procesów transformacji cyfrowej ochrony zdrowia poprzez dalszy rozwój usług cyfrowych w ochronie zdrowia” będąca elementem komponentu D „Efektywność, dostępność i jakość systemu ochrony zdrowia”.

Zakres usługi oraz warunki realizacji zostały opisane w tabelach poniżej.

Przeprowadzony audyt ma wykazać czy po realizacji projektu zwiększył się poziom bezpieczeństwa teleinformatycznego w odniesieniu do poziomu wynikającego z ankiety lub jest jego brak. Raport musi zawierać jasne stanowisko audytora w zakresie wykazania, że spożytkowane środki wpłynęły na podniesienie poziomu bezpieczeństwa.

Jako audyt zerowy, dokumentujący stan początkowy cyberbezpieczeństwa należy wykorzystać ankietę cyberbezpieczeństwa załączona do umowy o dofinansowanie.

Zakres usługi:

Lp.	PARAMETR/WARUNEK	WARTOŚĆ WYMAGANA	WARTOŚĆ OFEROWANEGO PARAMETRU, OPISAĆ (wypełnia Wykonawca)
1.	Wykonanie audytu końcowego zgodnie z dołączoną „Ankietą weryfikacji dojrzałości w zakresie cyberbezpieczeństwa” stanowiący załącznik do zapytania. Audyt ma zawierać wszystkie elementy ankiety	TAK	
2.	Audyt ma obejmować obszary, w których przetwarzane są dane osobowe wrażliwe, w tym kluczowe systemy informacji medycznej oraz infrastrukturę urządzeń medycznych (aparatura medyczna wraz z systemami je obsługującymi)	TAK	

3.	Audyt powinien obejmować niezbędną infrastrukturę teleinformatyczną podmiotu, w tym bezpieczeństwo takich elementów jak:		
a.	Kanały komunikacji jak np. poczta	TAK	
b.	Sieciowe urządzenia brzegowe wraz z zasadami segmentacji oraz przepływów	TAK	
c.	Kontrolery domeny	TAK	
d.	Platforma wirtualizacyjna	TAK	
e.	System zarządzania kopiami zapasowymi	TAK	
f.	Poprawność konfiguracji stacji roboczych oraz serwerów	TAK	
g.	Sposoby uwierzytelniania się użytkowników	TAK	
4.	Zakres prac audytorskich:	TAK	
	1. Raport podsumowujący wydany przez audytora wiodącego w formie drukowanej oraz w wersji elektronicznej. 2. Minimalny zakres informacji w tekście audytu: 2.1. Interpretacje zespołu audytorskiego wymagań określonych w ustawie o Krajowym Systemie Cyberbezpieczeństwa ze szczególnym odniesieniem się do niezbędnego zakresu stosowania wymagań formalnych bezpieczeństwa i ciągłości działania w organizacji i procesów kluczowych z wykluczeniem procesów merytorycznych 2.2. rekomendacje dla organizacji w zakresie wymagań polityk bezpieczeństwa informacji i audytu wymaganego ustawą. 2.3. rekomendacje działań korygujących lub naprawczych w systemie dokumentacyjnym w aktualnym polityk bezpieczeństwa informacji 2.4. rekomendacje działań korygujących lub naprawczych w systemie dokumentacyjnym w kontekście wymagań polityki ciągłości działania	Tak	

	<p>2.5.jeżeli wymagane, rekomendacje w zakresie infrastruktury sieciowej: jej architektury, konfiguracji, stosowanych zabezpieczeń, adekwatności do wymaganego/oczekiwanego poziomu bezpieczeństwa</p> <p>2.6.jeżeli wystąpią: rekomendacje w zakresie poprawy technologii oraz jakości wykonania dla infrastruktury sieciowej.</p> <p>2.7.porównanie stanu badanych pól działalności Szpitala opisanych w ankiecie ze stanem obecnym.</p> <p>3. Dokumentacja powykonawcza (w zakresie uzgodnionym z Zamawiającym(w 3 egzemplarzach w wersji papierowej oraz elektronicznej w ustalonym między stronami formacie (Zakres raportu w wersji edytowanej docx. Zestawienie tabelarycznej w postaci edytowalnego MS Excel, rysunki, schematy w postaci pdf) oraz prezentacji pptx dla Zarządu.</p>		
5.	<p>Kryteria oceny systemu:</p> <ol style="list-style-type: none"> 1. norma PN ISO/IEC 27001 2. norma PN ISO/IEC 22301 3. Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz.U. z 2018 r. poz. 1560, z 2019 r. poz. 2020) 4. Rozporządzenie Rady Ministrów z dnia 16 października 2018 r. w sprawie rodzajów dokumentacji dotyczącej cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej (Dz.U. z 2018 r., poz. 2080) 5. Rozporządzenie Ministra Cyfryzacji z dnia 10 września 2018 r. w sprawie warunków organizacyjnych i technicznych dla podmiotów świadczących usługi z zakresu cyberbezpieczeństwa oraz wewnętrznych struktur organizacyjnych operatorów usług kluczowych odpowiedzialnych za cyberbezpieczeństwa (Dz.U. z 2018 r., poz. 1780) 	Tak	
6.	Weryfikacja i analiza bezpieczeństwa dostępu do wewnętrznej infrastruktury sieciowej IT.	Tak	

<p>Weryfikacja i analiza jakościowa odporności infrastruktury IT na bezautoryzacyjne rozpoznanie jego składowych, w tym weryfikacja podatności serwisów DNS.</p> <p>Weryfikacja systemów oraz protokołów zarządzania i monitorowania infrastruktury IT.</p> <p>Weryfikacja jakościowa ochrony przed oprogramowaniem szkodliwym poprzez próby propagacji testowego oprogramowania szkodliwego. (zarówno z zewnątrz jak i od wewnątrz infrastruktury IT).</p> <p>Weryfikacja środków technicznych kontroli dostępu do systemów operacyjnych, w tym zabezpieczeń przed możliwością nieautoryzowanych instalacji oprogramowania.</p> <p>Weryfikacja i analiza danych przetwarzanych przez systemy logowania.</p> <p>Weryfikacja podatności logicznych środków kontroli dostępu wewnątrz Infrastruktury IT.</p> <p>Weryfikacja podatności systemów i sieci na ataki takie jak sniffing, spoofing, man-in-the-middle</p> <p>Weryfikacja na podstawie otwartości portów, podatności związanych z autoryzacją dostępu zdalnego do zasobów IT i ocena związanych z tym ryzyk.</p> <p>Weryfikacja bezautoryzacyjnego dostępu do informacji o rodzaju i wersji wykorzystywanego oprogramowania systemowego i usługowego.</p> <p>Weryfikacja arbitralnego i bezautoryzacyjnego zarządzania cyklem zmian systemów operacyjnych na urządzeniach infrastruktury IT.</p> <p>Rozpoznanie i ocena mechanizmów zarządzania aktualizacjami - w tym obecność systemów automatyzujących propagację poprawek bezpieczeństwa.</p> <p>Weryfikacja podatności na bezautoryzacyjne połączenia systemów VoIP.</p> <p>Weryfikacja podatności hostów na ataki w warstwie systemowej (przy wykorzystaniu exploitów).</p> <p>Weryfikacja podatności hostów na możliwość uzyskania nieautoryzowanego do-</p>		
---	--	--

<p> stępu do zasobów plikowych. Weryfikacja poufności przesyłu danych przetwarzanych na udostępnionych zasobach plikowych. Weryfikacja podatności ustawień hostów na możliwość uzyskania nieautoryzowanego zdalnego dostępu do kontroli treści przesyłanych przez przeglądarki www. Weryfikacja bezautoryzacyjnej dostępności do danych o czasie pracy, krytycznych systemów. Weryfikacja obecności domyślnych kont użytkowników oraz haseł. Weryfikacja bezpieczeństwa informacji zawartych w komunikatach systemów. Weryfikacja obecności podatnych algorytmów szyfrowania. Weryfikacja podatności systemów i aplikacji www w wewnętrznej infrastrukturze IT. Weryfikacja poufności przesyłania danych do wydruku. Analiza i ocena dodatkowych systemów bezpieczeństwa tj. dodatkowego oprogramowania antywirusowego, oprogramowania weryfikującego integralność systemów i gwarantującego audytowalność infrastruktury IT. Weryfikacja podatności systemu sieci wewnętrznej na zakłócenie/zablokowanie dostępności do usług i określenie zasięgu oraz zlokalizowanie fizycznego źródła ataku. Zebranie dostępnych wiadomości o obiekcie metodą pasywną. Wykorzystanie baz danych i narzędzi online: whois, dns, robtex, etc. Analiza informacji zawartych w nagłówkach odpowiedzi aplikacji www. Analiza informacji zawartych w odpowiedziach aplikacji www Próba wykrycia luk i podatności konfiguracyjnych. Analiza metadanych plików. Próba enumeracji zasobów danych. Próba przeprowadzenia ataku słownikowego na hasła użytkowników. Próba ujawnienia wycieków danych (obecność popularnych plików, analiza </p>		
--	--	--

<p>informacje o błędach, niewłaściwe nazewnictwo zasobów, wycieki kodu aplikacji).</p> <p>Próby wywołania błędów aplikacji (manipulacja przesyłanymi danymi, w tym:)</p> <p>Przesyłanie niepoprawnych danych.</p> <p>Przesyłanie nadmiarowych danych.</p> <p>Manipulacja parametrami oraz danymi nagłówkowymi zapytań</p> <p>Praktyczne sprawdzenie wykrytych podatności :</p> <p>Próba exploitacji z użyciem bazy posiadanych exploitów</p> <p>Weryfikacja nieautoryzowanego dostępu do testowanego systemu</p> <p>Weryfikacja informacji wrażliwych, uzyskanych w odpowiedziach systemu.</p> <p>Weryfikacja reakcji zabezpieczeń testowanego systemu, na przeprowadzane próby ataku.</p> <p>Analiza bezpieczeństwa systemu poczty elektronicznej będący szczególnym przypadkiem audytu teleinformatycznego i rozszerzający zakres audytu teleinformatycznego.</p> <p>Weryfikację oprogramowania AV poczty elektronicznej na rozsyłanie zagrożeń zawierających w treści zagrożenia, przesyłanych z wewnątrz i zewnątrz infrastruktury IT</p> <p>Badanie podatności systemu poczty na próby bezautoryzacyjnego dostępu do skrzynek poczty elektronicznej pracowników</p> <p>Badanie podatności systemu dostępu przez www do poczty elektronicznej.</p> <p>Analiza bezpieczeństwa usługi katalogowej Active Directory będący szczególnym przypadkiem audytu teleinformatycznego i rozszerzający zakres audytu teleinformatycznego.</p> <p>Weryfikację bezpieczeństwa transmisji danych pomiędzy serwerem a stacjami roboczymi.</p> <p>Weryfikację reakcji i czasu reakcji na atak account lockout w domenie.</p> <p>Weryfikację bezpieczeństwa poufności przesyłanych danych potrzebnych do au-</p>		
--	--	--

	toryzacji, z urządzeń zintegrowanych z AD. Weryfikację bezpieczeństwa poufności instrukcji GPO pod kątem ujawniania krytycznych informacji o systemach i wycieku danych.		
7.	Audyt fizyczny i środowiskowy, którego celem jest weryfikacja skutecznej ochrony fizycznej i środowiskowej zasobów. W skład tego audytu wchodzi: Weryfikacja granic obszaru bezpiecznego. Weryfikacja zabezpieczeń wejścia/wyjścia. Weryfikacja systemów zabezpieczeń pomieszczeń i urządzeń. Weryfikacja bezpieczeństwa okablowania strukturalnego. Weryfikacja systemów chłodzenia. Weryfikacja systemów alarmowych.		

Zakres weryfikacji ankiety dojrzałości:

1) System kopii zapasowych

Lp.	Nazwa kryterium	Czy spełnione? (Tak / Nie)	Czy obligatoryjne?
1.	Wdrożony system tworzy odmiejszczone kopie zapasowe. System posiada aktualne wsparcie producenta oraz wykonuje kopie kluczowych systemów podmiotu.		Tak
2.	Infrastruktura systemu backupu jest odseparowana od systemu produkcyjnego		Tak
3.	Przeprowadzono testy odtworzenia systemu i potwierdzono skuteczność/poprawność odtworzenia		Tak
4.	Podmiot posiada dokumentację powdrożeniową systemu backupu.		Tak
5.	Administratorzy systemu backupu podmiotu odbyli instruktaż z obsługi systemu kopii zapasowych.		Tak
6.	Wdrożono procedury backupowe oraz odtworzeniowe i procedury te są stosowane.		Nie
7.	Tworzone są i weryfikowane raporty z cyklicznego wykonywania odmiejszczonej kopii zapasowej.		Nie
8.	Podmiot cyklicznie odtwarza dane z kopii zapasowych w celu weryfikacji poprawności. Odtworzenia testowe potwierdzone są protokołem.		Nie

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 odmiejszczonej 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 skuteczność wprowadzonych zabezpieczeń i potwierdzającego zgodność konfiguracji z dokumentacją – dla usług testów bezpieczeństwa.
- Wyciąg z umowy obejmujący zakres usługi – dla usług utrzymaniowych

2) Zapory sieciowe

Lp.	Nazwa kryterium	Czy spełnione? (Tak / Nie)	Czy obligatoryjne?
1.	Wdrożono moduł ochrony przed złośliwym oprogramowaniem dla ruchu z/do Internetu, posiadający aktualne wsparcie.		Tak
2.	Wdrożono i włączono moduł IPS/IDS przynajmniej dla ruchu z/do Internetu, posiadający aktualne wsparcie.		Tak
3.	Wdrożono i włączono moduły filtrowania zawartości oraz reguły filtrowania po kategorii treści.		Tak
4	Na brzegu sieci zainstalowany Firewall, a sama sieć podzielona jest na podsieci.		Tak
5.	Kluczowe aplikacje/systemy, w szczególności dostępne publicznie chronione są za pomocą firewalla aplikacyjnego (WAF) z włączonymi modułami ochrony aplikacji, ochrony DoS/DDoS.		Nie
6.	Pliki pobierane z sieci Internet podlegają analizie w izolowanych środowiskach typu Sandbox.		Nie
7.	Domyślne hasła przekazane przy odbiorze zostały zmienione i objęte procedurą zarządzania hasłami w organizacji.		Tak
8.	Nieużywane porty, usługi oraz konta zostały wyłączone.		Tak
9.	Dostęp do panelu zarządzania zaporą sieciową został ograniczony jedynie dla wyznaczonych osób zgodnie z obowiązującą procedurą nadawania uprawnień oraz dostępny jest wyłącznie z wybranej podsieci.		Tak
10.	Wdrożona została procedura cyklicznego wykonywania kopii zapasowych konfiguracji urządzenia (lub po każdej zmianie reguł i wersji) .Procedura ta jest stosowana.		Tak

11.	Administratorzy posiadają kompetencje w postaci odbytego instruktażu stanowiskowego i/lub odbytych szkoleń z obsługi dedykowanego systemu Firewall.		Tak
-----	---	--	-----

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.

3) Ochrona poczty e-mail

Lp.	Nazwa kryterium	Czy spełnione? (Tak / Nie)	Czy obligatoryjne?
1.	Wdrożono mechanizmy ochrony poczty SPF, DMARC, DKIM.		Tak
2.	Wdrożono ochronę antyspam oraz ochronę przed złośliwym oprogramowaniem, z aktualnym wsparciem producenta i aktualnymi sygnaturami.		Tak
3.	Przeprowadzono testy wdrożonych mechanizmów ochrony poczty, które potwierdziły poprawne ich działanie.		Tak
4.	Wdrożono obowiązkowy drugi składnik uwierzytelniający (2FA) dla poczty dostępnej z sieci publicznej.		Tak
5.	Uwierzytelnianie do poczty dostępnej publicznie jest zgodne ze standardem FIDO2.		Nie
6.	Wdrożono zasady bezpiecznego wykorzystania poczty w organizacji.		Nie
7.	Wiadomości przychodzące z zewnątrz oznaczane są dedykowanym banerem.		Nie
8.	Administratorzy posiadają kompetencje w postaci odbytego instruktażu stanowiskowego z obsługi dedykowanego systemu lub usługi.		Tak
9.	Kopia bezpieczeństwa poczty jest regularnie wykonywana.		Tak

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 z testowym odtworzeniem. Raport zawierający informacje o aktualizacji systemu pocztowego wraz z jego ochroną

4) Segmentacja sieci

Lp.	Nazwa kryterium	Czy spełnio- ne? (Tak / Nie)	Czy obligatoryj- ne?
1.	Wdrożono segmentację sieciową (na poziomie VLANów) zapewniającą odseparowanie sieci biurowej, systemów serwerowych, systemu kopii zapasowych, urządzeń medycznych, sieci gościnnej.		Tak
2.	Wdrożono reguły bezpieczeństwa pomiędzy segmentami sieci oparte na zasadzie minimalnego niezbędnego dostępu.		Tak
3.	Dokumentacja architektury sieciowej jest sporządzona i aktualizowana.		Nie
4.	Wszystkie podłączane do sieci urządzenia są identyfikowane, uwierzytelniane oraz autoryzowane.		Nie

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.

5) Ochrona stacji roboczych oraz serwerów (rozwiązania klasy EDR)

Lp.	Nazwa kryterium	Czy spełnio- ne? (Tak / Nie)	Czy obligatoryj- ne?
1.	Wdrożono rozwiązanie ochrony przed złośliwym oprogramowaniem z aktualnym wsparciem producenta.		Tak
2.	Wdrożono rozwiązanie klasy EDR, obejmujące wszystkie wspierane przez producenta oprogramowania stacje robocze oraz serwery.		Tak
3.	Wdrożono rozwiązanie klasy XDR, obejmujące wszystkie wspierane przez producenta oprogramowania stacje robocze i serwery oraz zbierające i analizujące dane również z innych źródeł.		Nie
4.	Dla serwerów oraz stacji roboczych nieobjętych ochroną została wykonana analiza ryzyka.		Tak
5.	Osoby administrujące systemami ochrony stacji i serwerów posiadają odpowiednie kompetencje potwierdzone odbytym		Tak

	szkoleniem.		
--	-------------	--	--

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.

6) Zarządzanie podatnościami

Lp.	Nazwa kryterium	Czy spełnione? (Tak / Nie)	Czy obligatoryjne?
1.	Wdrożono system automatycznego (sieciowego i/lub agentowego) skanowania i identyfikacji podatności.		Nie
2.	Skanowanie podatności obejmuje przynajmniej kluczowe stacje robocze, serwery oraz urządzenia sieciowe.		Nie
3.	Skanowanie podatności obejmuje proces uwierzytelnienia się do poziomu systemu operacyjnego skanowanego hostu.		Nie
4.	Skanowanie podatności obejmuje ocenę poprawności konfiguracji bezpieczeństwa skanowanego hostu.		Nie
5.	Ocena ryzyka podatności uwzględnia inne czynniki niż system klasyfikacji CVSS.		Nie
6.	Ustalono czasy reakcji na zidentyfikowane podatności.		Nie

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.

7) System zarządzania bezpieczeństwem informacji

Lp.	Nazwa kryterium	Czy spełnione? (Tak / Nie)	Czy obligatoryjne?
1.	Wdrożono politykę zarządzania dostępem i uprawnieniami.		Tak
2.	Wdrożono politykę kryptografii z uwzględnieniem zalecanych dopuszczalnych protokołów szyfrowania.		Tak
3.	Wdrożono politykę zarządzania podatnościami		Tak
4.	Wdrożono politykę zarządzania ryzykiem z uwzględnieniem obszaru cyberbezpieczeństwa		Tak
5.	Wdrożono politykę logowania zdarzeń z uwzględnieniem aplikacji, sieci, serwerów, bramy brzegowej, kontrolerem domeny.		Tak
6.	Wdrożono politykę kopii bezpieczeństwa.		Tak

7.	Wdrożono politykę zarządzania incydentami bezpieczeństwa.		Tak
8.	Wdrożono politykę zarządzania ciągłością działania.		Tak
9.	Wdrożono politykę ochrony danych osobowych z uwzględnieniem przetwarzania danych medycznych		Tak

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 jego realizacji, monitorowania i okresowych przeglądów.

- Lista opracowanej dokumentacji wraz z opisem
- Potwierdzenie uczestnictwa w szkoleniach – dla usług szkoleniowych

8) Szkolenia z zakresu podnoszenia świadomości w obszarze cyberbezpieczeństwa (cyberhigieny)

Lp.	Nazwa kryterium	Czy spełnione? (Tak / Nie)	Czy obligatoryjne?
1.	Odbycie szkolenia przez kadrę kierowniczą, w okresie ostatniego roku, minimum w zakresie: <ul style="list-style-type: none"> • Podstaw prawnych w obszarze cyberbezpieczeństwa • Typów ataków • Reagowania na incydenty • Wykonywania badań bezpieczeństwa • Roli kadry zarządzającej w procesach bezpieczeństwa 		Tak
2.	Odbycie szkolenia przez kadrę biurową i medyczną – min. 75% pracowników pracujących na systemach informatycznych szpitala, w okresie ostatniego roku, minimum w zakresie: <ul style="list-style-type: none"> • Podstawowych zasad cyberhigieny • Typów ataków wraz z przykładami • Reagowania na incydenty 		Tak

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

9) Usługi zarządzane bezpieczeństwem

Lp.	Nazwa kryterium	Czy spełnione? (Tak / Nie)	Czy obligatoryjne?
1.	Systemy teleinformatyczne jak i infrastruktura teleinformatyczna monitorowana jest całodobowa pod kątem bezpieczeństwa		Nie
2.	Przygotowano i przetestowano indywidualne procedury reagowania na incydenty bezpieczeństwa dla najbardziej powszechnych i najczęściej pojawiających się zdarzeń		Nie

3.	Utrzymywany jest centralny system klasy SIEM lub system centralnej kolekcji zdarzeń/logów gromadzący istotne z punktu widzenia zdarzenia bezpieczeństwa z infrastruktury teleinformatycznej oraz aplikacji i systemów,		Nie
4.	Kluczowe aplikacje, systemy oraz infrastruktura teleinformatyczna testowana jest pod kątem bezpieczeństwa		Nie
5.	Ubezpieczenie od ryzyk cybernetycznych stosowane jest jako element uzupełniający zarządzania ryzykiem.		Nie

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.

9) Uwierzytelnienie i autoryzacja do systemów

Lp.	Nazwa kryterium	Czy spełnione? (Tak / Nie)	Czy obligatoryjne?
1.	Wszystkie krytyczne systemy w organizacji wymagają użycia drugiego składnika uwierzytelniania lub uwierzytelniania bezhasłowego.		Nie
2.	Każda osoba w organizacji ma obowiązek korzystania z drugiego składnika uwierzytelniania lub uwierzytelniania bezhasłowego (jeżeli jest dostępny).		Nie
3.	W przypadku wykorzystywania systemu pojedynczego logowania dla dostępu do systemów i aplikacji, uwierzytelnienie użytkownika odbywa się z wykorzystaniem metod wieloskładnikowych lub uwierzytelniania bezhasłowego.		Nie
4.	Wyłączono możliwość używania SMS-ów jako metody uwierzytelniania.		Nie
5.	Uwierzytelnianie do krytycznych systemów i aplikacji w organizacji jest zgodne ze standardem FIDO2.		Nie
6.	Wszystkie połączenia zdalne wymagają wieloskładnikowego uwierzytelniania.		Nie
7.	Uwierzytelnianie użytkownika uwzględnia jego kontekst np. urządzenie z którego następuje logowanie.		Nie

Kryteria akceptacji do oceny przy audycie końcowym w obszarze cyberbezpieczeństwa:

- Dokumentacja powykonawcza wdrożonych rozwiązań uwierzytelniających wraz z zabezpieczeniami – dla zakupu urządzeń i oprogramowania oraz usług wdrożeniowych.
- Potwierdzenie uczestnictwa w szkoleniach – dla usług szkoleniowych.

Termin realizacji zadania - do dnia 03.07.2026 r.

UWAGA:

1. W przypadku zastosowania przez Zamawiającego w opisie przedmiotu zamówienia odniesień lub nazw specyfikacji technicznych, aprobat, technologii, funkcjonalności lub norm, Zamawiający dopuszcza zaoferowanie rozwiązań co najmniej równoważnych z opisywanymi. Wykonawca, który w celu realizacji Zamówienia powołuje się na rozwiązania co najmniej równoważne z opisywanym przez Zamawiającego, jest obowiązany wykazać, że oferowane przez Wykonawcę rozwiązania spełniają wymagania określone przez Zamawiającego.

2. Jeżeli w jakimkolwiek dokumencie postępowania znajduje się jakikolwiek znak towarowy, znak handlowy jakiegoś wyrobu, nazwa własna (handlowa), patent czy pochodzenie – należy przyjąć, że Zamawiający podał taki opis ze wskazaniem na typ i dopuszcza zastosowanie materiałów, urządzeń, sprzętu i wyposażenia o co najmniej równoważnych parametrach technicznych w odniesieniu do parametrów podanych pod pojęciem typu. Wykonawca, który w celu realizacji Zamówienia powołuje się na rozwiązania co najmniej równoważne, jest obowiązany wykazać, że oferowane przez Wykonawcę rozwiązania spełniają wymagania określone przez Zamawiającego.

..... dnia
(miejscowość)

.....
(podpis(y) osoby (osób) upoważnionej
do występowania w imieniu Wykonawcy)