

OPIS PRZEDMIOTU ZAMÓWIENIA - PAKIET 2

A. ZAKRES ZAMÓWIENIA

Przedmiotem zamówienia jest przeprowadzenie audytu na zgodność z normą ISO 27001 wraz z testami bezpieczeństwa oraz weryfikacja zgodności Systemu Zarządzania Bezpieczeństwem Informacji funkcjonującego w audytowanej jednostce (Szpitalu) z wymaganiami normy **ISO/IEC 27001:2022**, oraz ustawy o krajowym systemie cyberbezpieczeństwa (UKSC) z dnia 5 lipca 2018 r. (Dz. U. z 2026 r. poz. 20 z późn. zm)

Zakres zamówienia objęty jest Wniskiem o wsparcie w zakresie:

Zadanie 3: Działania zwiększające poziom cyberbezpieczeństwa szpitala

Koszt 3.22 - Audyt na zgodności z ISO 27001 z testami

B. TERMIN REALIZACJI

Wykonawca zobowiązany jest do wykonania przedmiotu umowy w terminie od 21 czerwca 2026 roku,
nie później jednak niż do dnia 3 lipca 2026 roku.

C. GWARANCJA JAKOŚCI

W ramach zamówienia wykonawca udzieli na wykonane usługi gwarancji jakości na okres nie krótszy niż 12 miesięcy od daty podpisania protokołu odbioru prawidłowo wykonanego przedmiotu zamówienia.

D. OPIS MINIMALNYCH WYMAGAŃ FUNKCYJONALNYCH I TECHNICZNYCH

I. Audytu na zgodność z normą ISO 27001

Przedmiotem tej części zamówienia jest przeprowadzenie audytu zgodności Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) funkcjonującego w Szpitalu z wymaganiami normy ISO/IEC 27001:2022, wraz z oceną wdrożenia zabezpieczeń określonych w Załączniku A normy oraz przygotowaniem raportu końcowego zawierającego wyniki, niezgodności, obserwacje i rekomendacje.

1. Wykonawca zobowiązany jest do przeprowadzenia prac w oparciu o:
 - 1.1. Normę ISO/IEC 27001:2022.
 - 1.2. Ustawę z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.
 - 1.3. Rozporządzenie Rady Ministrów w sprawie progów uznania incydentu za poważny.
 - 1.4. Standardy prowadzenia audytu zgodne z ISO 19011:2018
2. Zakres audytu
 - 2.1. Audyt musi obejmować następujące obszary:
 - 2.2. Zabezpieczenia organizacyjne: polityka bezpieczeństwa, zarządzanie ryzykiem, relacje z dostawcami, zarządzanie incydentami oraz ciągłość działania.
 - 2.3. Zasoby ludzkie: świadomość pracowników, zasady zatrudniania i zwalniania, praca zdalna.
 - 2.4. Zabezpieczenia fizyczne: strefy bezpieczeństwa, dostęp fizyczny, zabezpieczenie serwerowni, ochrona przed zagrożeniami środowiskowymi oraz utylizacja nośników.
 - 2.5. Zabezpieczenia technologiczne: kontrola dostępu, kopie zapasowe, ochrona przed złośliwym oprogramowaniem, bezpieczeństwo sieci (LAN/WAN), kryptografia oraz bezpieczny rozwój systemów.
3. Wykonawca w ramach prac musi przeprowadzić:
 - 3.1. Analizę dokumentacji SZBI (polityki, procedury, rejestry).
 - 3.2. Wywiady z pracownikami w celu weryfikacji ich świadomości w zakresie cyberbezpieczeństwa.

- 3.3. Testy podatnościowe infrastruktury (zgodnie z zakresem podatności opisanym w rozdziale II), w tym:
 - 3.3.1.1. Sieć LAN: skanowanie hostów pod kątem luk (zgodnie z bazą CVE), weryfikacja konfiguracji stacji roboczych i urządzeń sieciowych.
 - 3.3.1.2. Sieć WAN: weryfikacja zabezpieczeń punktu styku z Internetem, testy VPN i uwierzytelniania dwuskładnikowego (2FA).
 - 3.3.1.3. Strona Internetowa: weryfikacja certyfikatów SSL/TLS (np. poprzez SSL Labs) oraz podatności witryny.
- 3.4. Weryfikację mechanizmów kontrolnych, w tym skuteczności Firewall, IDS/IPS oraz filtrowania treści.
4. Raport z audytu (Protokół pokontrolny) musi posiadać strukturę obejmującą co najmniej:
 - 4.1. Metrykę audytu i opis metodyki z klasyfikacją nieprawidłowości (Krytyczny, Wysoki, Średni, Niski).
 - 4.2. Podsumowanie dla kierownictwa zawierające statystykę wykrytych podatności i najważniejsze niezgodności.
 - 4.3. Szczegółową ocenę zgodności (%) dla każdego z audytowanych obszarów (zgodnie z listą 35 obszarów w źródle).
 - 4.4. Opis zidentyfikowanych nieprawidłowości wraz z przypisanym priorytetem.
 - 4.5. Konkretnie rekomendacje naprawcze, w tym wymagania dotyczące prowadzenia rejestrów aktywów, incydentów, ryzyk, procesów, upoważnień, kopii zapasowych, informacji oraz systemów.
 - 4.6. Opinię audytorską (Pozytywna/Negatywna) wraz z uzasadnieniem.
 - 4.7. Załączniki techniczne z wynikami skanowania podatności, zawierające nazwy luk, opisy, rekomendowane rozwiązania oraz odnośniki do wpisów CVE
5. Wymagania wobec zespołu audytowego
 - 5.1. W skład zespołu audytowego muszą wchodzić co najmniej dwie osoby posiadające potwierdzone kompetencje zgodnie z Rozporządzeniem Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu (Dz.U. 2018 poz. 1999) tj. 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 (Dz. U. z 2016 r. poz. 542), w zakresie certyfikacji osób.

II. Testy Podatności

1. Wymagany minimalny zakres testów
 - 1.1. Wykonanie skanów otwartych portów w adresacji publicznej audytowanego podmiotu.
 - 1.2. Wykorzystanie dedykowanego oprogramowania do wykrywania podatności zasilonego najnowszą bazą znanych podatności.
 - 1.3. Wykonanie testów usług i infrastruktury dostępnych z Internetu, sieci wewnętrznej, usługi katalogowej, platformy wirtualizacyjnej, kanałów komunikacji oraz poprawności konfiguracji próbki serwerów i stacji roboczych
 - 1.4. Wykonanie skanów niewuierzytelnionych:
 - 1.4.1.usług i infrastruktury dostępnych z Internetu,
 - 1.4.2.sieci wewnętrznej, usługi katalogowej, platformy wirtualizacyjnej,
 - 1.4.3.kanałów komunikacji oraz poprawności konfiguracji próbki serwerów i stacji roboczych
 - 1.5. Testy podatności środowiska teleinformatycznego Zamawiającego muszą zweryfikować istnienie minimum następujących rodzin podatności:

lp.	podatność	lp.	podatność
1.	AIX Local Security Checks	28.	Mobile Devices
2.	Amazon Linux Local Security Checks	29.	Netware

3.	Backdoors	30.	NewStart CGSL Local Security Checks
4.	Brute force attacks	31.	Oracle Linux Local Security Checks
5.	CGI abuses	32.	OracleVM Local Security Checks
6.	CGI abuses : XSS	33.	Palo Alto Local Security Checks
7.	CISCO	34.	Peer-To-Peer File Sharing
8.	CentOS Local Security Checks	35.	PhotonOS Local Security Checks
9.	DNS	36.	Policy Compliance
10.	Databases	37.	Port scanners
11.	Debian Local Security Checks	38.	RPC
12.	Default Unix Accounts	39.	Red Hat Local Security Checks
13.	Denial of Service	40.	SMTP problems
14.	F5 Networks Local Security Checks	41.	SNMP
15.	FTP	42.	Scientific Linux Local Security Checks
16.	Fedora Local Security Checks	43.	Service detection
17.	Firewalls	44.	Settings
18.	FreeBSD Local Security Checks	45.	Slackware Local Security Checks
19.	Gain a shell remotely	46.	Solaris Local Security Checks
20.	General	47.	SuSE Local Security Checks
21.	Gentoo Local Security Checks	48.	Ubuntu Local Security Checks
22.	HP-UX Local Security Checks	49.	VMware ESX Local Security Checks
23.	Huawei Local Security Checks	50.	Virtuozzo Local Security Checks
24.	Junos Local Security Checks	51.	Web Servers
25.	MacOS X Local Security Checks	52.	Windows
26.	Mandriva Local Security Checks	53.	Windows : Microsoft Bulletins
27.	Misc.	54.	Windows : User management

2. Zakres Raportu z testów bezpieczeństwa

- 2.1. ExecutiveSummary – główne konkluzje
- 2.2. Główne rekomendacje
- 2.3. Risk Rating
- 2.4. Metodologia i kryteria testowania
- 2.5. Wykorzystane narzędzia w trakcie prowadzenia skanów
- 2.6. Wykaz zidentyfikowanych podatności wraz z odpowiadającym im kodem CVE (CommonVulnerabilityEnumaration) oraz odnośnikiem do opisu luki.
- 2.7. Podatności pogrupowane według ryzyka, zgodnie ze standardem CVSS (CommonVulnerabilityScoring System).
- 2.8. Rekomendacje związane z możliwym usunięciem wykrytych podatności.

III. Weryfikacja dojrzałości infrastruktury informatycznej Zamawiającego w zakresie cyberbezpieczeństwa

Zamawiający wymaga od Wykonawcy przeprowadzenia weryfikacji dojrzałości infrastruktury informatycznej Zamawiającego w zakresie szczegółowo opisanym poniżej oraz sporządzenia i przedłożenia Zamawiającemu Raportu z przeprowadzonej weryfikacji, którego zakres dla każdego z weryfikowanych obszarów jest wyspecyfikowany poniżej.

Wymagania co do zakresu weryfikacji oraz zawartości Raportu z przeprowadzonej weryfikacji:

1. System kopii zapasowych

- 1.1. Obszary podlegające weryfikacji:
 - 1.1.1. Wdrożony system tworzy odmiejscowione kopie zapasowe. System posiada aktualne wsparcie producenta oraz wykonuje kopie kluczowych systemów podmiotu.
 - 1.1.2. Infrastruktura systemu backupu jest odseparowana od systemu produkcyjnego

- 1.1.3. Przeprowadzono testy odtworzenia systemu i potwierdzono skuteczność/poprawność odtworzenia
- 1.1.4. Podmiot posiada dokumentację powdrożeniową systemu backupu.
- 1.1.5. Administratorzy systemu backupu podmiotu odbyli instruktaż z obsługi systemu kopii zapasowych.
- 1.2. Zawartość Raportu z weryfikacji:
- 1.2.1. Zestawienie wszystkich kluczowych i pomocniczych systemów objętych systemem kopii zapasowych – dla zakupu sprzętu i oprogramowania oraz usług wdrożeniowych.
- 1.2.2. Dokument zawierający wymagania dotyczące częstotliwości wykonywania kopii zapasowych – dla zakupu sprzętu i oprogramowania oraz usług wdrożeniowych.
- 1.2.3. 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.
- 1.2.4. Raport z testów funkcjonalnych i niefunkcjonalnych działania systemu backupu – dla zakupu sprzętu i oprogramowania oraz usług wdrożeniowych.
- 1.2.5. Potwierdzenie uczestnictwa na szkoleniach z zakresu obsługi systemu kopii zapasowej – w zakresie usług szkoleniowych.
- 1.2.6. Wyniki testu potwierdzającego skuteczność wprowadzonych zabezpieczeń i potwierdzającego zgodność konfiguracji z dokumentacją – dla usług testów bezpieczeństwa.
- 1.2.7. Wyciąg z umowy obejmujący zakres usługi – dla usług utrzymaniowych
- 2. Zapory sieciowe**
- 2.1. Obszary podlegające weryfikacji:
- 2.1.1. Wdrożono moduł ochrony przed złośliwym oprogramowaniem dla ruchu z/do Internetu, posiadający aktualne wsparcie.
- 2.1.2. Wdrożono i włączono moduł IPS/IDS przynajmniej dla ruchu z/do Internetu, posiadający aktualne wsparcie.
- 2.1.3. Wdrożono i włączono moduły filtrowania zawartości oraz reguły filtrowania po kategorii treści.
- 2.1.4. Na brzegu sieci zainstalowany Firewall, a sama sieć podzielona jest na podsieci.
- 2.1.5. Domyślne hasła przekazane przy odbiorze zostały zmienione i objęte procedurą zarządzania hasłami w organizacji.
- 2.1.6. Nieużywane porty, usługi oraz konta zostały wyłączone.
- 2.1.7. 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.
- 2.1.8. Wdrożona została procedura cyklicznego wykonywania kopii zapasowych konfiguracji urządzenia (lub po każdej zmianie reguł i wersji) .Procedura ta jest stosowana.
- 2.1.9. Administratorzy posiadają kompetencje w postaci odbytego instruktażu stanowiskowego i/lub odbytych szkoleń z obsługi dedykowanego systemu Firewall. Tak
- 2.2. Zawartość Raportu z weryfikacji:
- 2.2.1. Dokumentacja powykonawcza wdrożonych zapór sieciowych wraz z zabezpieczeniami – dla zakupu sprzętu i oprogramowania oraz usług wdrożeniowych.
- 2.2.2. Wyniki testu potwierdzającego skuteczność wprowadzonych zabezpieczeń i potwierdzającego zgodność konfiguracji z dokumentacją – dla usług testów bezpieczeństwa.
- 2.2.3. Potwierdzenie uczestnictwa na szkoleniach z zakresu obsługi zainstalowanych zapór sieciowych – dla usług szkoleniowych.
- 2.2.4. Wyciąg z umowy obejmujący zakres usługi – dla usług utrzymaniowych.

3. Ochrona poczty e-mail

3.1. Obszary podlegające weryfikacji:

- 3.1.1. Wdrożono mechanizmy ochrony poczty SPF, DMARC, DKIM.
- 3.1.2. Wdrożono ochronę antyspam oraz ochronę przed złośliwym oprogramowaniem, z aktualnym wsparciem producenta i aktualnymi sygnaturami.
- 3.1.3. Przeprowadzono testy wdrożonych mechanizmów ochrony poczty, które potwierdziły poprawne ich działanie.
- 3.1.4. Wdrożono obowiązkowy drugi składnik uwierzytelniający (2FA) dla poczty dostępnej z sieci publicznej.
- 3.1.5. Administratorzy posiadają kompetencje w postaci odbytego instruktażu stanowiskowego z obsługi dedykowanego systemu lub usługi.
- 3.1.6. Kryteria akceptacji do oceny przy audycie końcowym w obszarze cyberbezpieczeństwa.

3.2. Zawartość Raportu z weryfikacji:

- 3.2.1. Opis sposobu ochrony poczty wraz z dokumentacją systemów ochrony poczty
- 3.2.2. 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/>
- 3.2.3. Wynik testu potwierdzającego wdrożenie obowiązkowego drugiego składnika uwierzytelniającego (2FA) dla poczty elektronicznej dostępnej publicznie.
- 3.2.4. Raport z wykonania backupu poczty elektronicznej wraz z testowym odtworzeniem.
- 3.2.5. Raport zawierający informacje o aktualizacji systemu pocztowego wraz z jego ochroną

4. Segmentacja sieci

4.1. Obszary podlegające weryfikacji:

- 4.1.1. Wdrożono segmentację sieciową (na poziomie VLANów) zapewniającą odseparowanie sieci biurowej, systemów serwerowych, systemu kopii zapasowych, urządzeń medycznych, sieci gościnnej.
- 4.1.2. Wdrożono reguły bezpieczeństwa pomiędzy segmentami sieci oparte na zasadzie minimalnego niezbędnego dostępu.

4.2. Zawartość Raportu z weryfikacji:

- 4.2.1. Dokument zawierający wymagania dotyczące podziału sieci wraz ze sposobem implementacji – dla zakupu sprzętu, oprogramowania oraz usług wdrożeniowych.
- 4.2.2. Dokumentacja sposobu identyfikowania, uwierzytelniania i autoryzacji urządzeń podłączanych do sieci – dla zakupu oprogramowania.
- 4.2.3. Wynik weryfikacji zgodności konfiguracji z dokumentacją – dla zakupu sprzętu, oprogramowania oraz usług wdrożeniowych.
- 4.2.4. Potwierdzenie uczestnictwa na szkoleniach z zakresu obsługi zainstalowanych systemów ochrony sieciowej – dla usług szkoleniowych
- 4.2.5. Wyciąg z umowy obejmujący zakres usługi – dla usług utrzymaniowych.
- 4.2.6. 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)

5.1. Obszary podlegające weryfikacji:

- 5.1.1. Wdrożono rozwiązanie ochrony przed złośliwym oprogramowaniem z aktualnym wsparciem producenta.
- 5.1.2. Wdrożono rozwiązanie klasy EDR, obejmujące wszystkie wspierane przez producenta oprogramowania stacje robocze oraz serwery.
- 5.1.3. Dla serwerów oraz stacji roboczych nieobjętych ochroną została wykonana analiza ryzyka.
- 5.1.4. Osoby administrujące systemami ochrony stacji i serwerów posiadają odpowiednie kompetencje potwierdzone odbytym szkoleniem.

5.2. Zawartość Raportu z weryfikacji:

- 5.2.1. 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.
- 5.2.2. Wyciąg z umowy obejmujący zakres usługi – dla usług utrzymaniowych.
- 5.2.3. Potwierdzenie uczestnictwa na szkoleniach z zakresu obsługi systemu – dla usług szkoleniowych.

6. System zarządzania bezpieczeństwem informacji

6.1. Obszary podlegające weryfikacji:

- 6.1.1. Wdrożono politykę zarządzania dostępem i uprawnieniami.
- 6.1.2. Wdrożono politykę kryptografii z uwzględnieniem zalecanych dopuszczalnych protokołów szyfrowania.
- 6.1.3. Wdrożono politykę zarządzania podatnościami
- 6.1.4. Wdrożono politykę zarządzania ryzykiem z uwzględnieniem obszaru cyberbezpieczeństwa
- 6.1.5. Wdrożono politykę logowania zdarzeń z uwzględnieniem aplikacji, sieci, serwerów, bramy brzegowej, kontrolerem domeny.
- 6.1.6. Wdrożono politykę kopii bezpieczeństwa.
- 6.1.7. Wdrożono politykę zarządzania incydentami bezpieczeństwa.
- 6.1.8. Wdrożono politykę zarządzania ciągłością działania.
- 6.1.9. Wdrożono politykę ochrony danych osobowych z uwzględnieniem przetwarzania danych medycznych

6.2. Zawartość Raportu z weryfikacji:

- 6.2.1. 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.
- 6.2.2. Lista opracowanej dokumentacji wraz z opisem
- 6.2.3. Potwierdzenie uczestnictwa w szkoleniach – dla usług szkoleniowych.

7. Szkolenia z zakresu podnoszenia świadomości w obszarze cyberbezpieczeństwa (cyberhigieny)

7.1. Obszary podlegające weryfikacji:

- 7.1.1. Odbycie szkolenia przez kadrę kierowniczą, w okresie ostatniego roku, minimum w zakresie:
 - 7.1.1.1. Podstaw prawnych w obszarze cyberbezpieczeństwa
 - 7.1.1.2. Typów ataków
 - 7.1.1.3. Reagowania na incydenty
 - 7.1.1.4. Wykonywania badań bezpieczeństwa
 - 7.1.1.5. Roli kadry zarządzającej w procesach bezpieczeństwa
- 7.1.2. Odbycie szkolenia przez kadrę biurową i medyczną – min. 75% pracowników pracujących na systemach informatycznych szpitala, w okresie ostatniego roku, minimum w zakresie:
 - 7.1.2.1. Podstawowych zasad cyberhigieny
 - 7.1.2.2. Typów ataków wraz z przykładami
 - 7.1.2.3. Reagowania na incydenty

7.2. Zawartość Raportu z weryfikacji:

- 7.2.1. Konspekt programu szkoleń
- 7.2.2. Potwierdzenie uczestnictwa w szkoleniach co najmniej 75% pracowników szpitala, pracujących na stacjach roboczych – oświadczenie dyrektora szpitala.