

Załącznik nr 1 do OPZ dot. zapytania nr DZ/DI-72-22/26
Ankieta weryfikacji dojrzałości w zakresie cyberbezpieczeństwa
1) System kopii zapasowych

Lp.	Nazwa kryterium	Czy spełnione? (Tak / Nie)	Czy obligatoryjne?
1.	Wdrożony system tworzy odmiejscowione 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 odmiejscowionej 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 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 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.	Nie używane 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
10.	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 spełnione? (Tak / Nie)	Czy obligatoryjne?
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 spełnione? (Tak / Nie)	Czy obligatoryjne?
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

Lp.	Nazwa kryterium	Czy spełnione? (Tak / Nie)	Czy obligatoryjne?
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 szkoleniem.		Tak

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

Lp.	Nazwa kryterium	Czy spełnione? (Tak / Nie)	Czy obligatoryjne?
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 usług 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.

10) 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.