KOPERNIK

WOJEWÓDZKI SZPITAL SPECJALISTYCZNY
im. M. Kopernika w Łodzi
Dział Zamówień Publicznych
tel. 042 689 58 19, 59 11, faks 042 689 54 09

EZ.263.236.1964.2015.AO

Łódź, dnia 23.12.2015 r.
Numer sprawy: **236/ZP/15**

dotyczy: postępowania o udzielenie zamówienia publicznego prowadzonego w trybie przetargu nieograniczonego o wartości powyżej 30 000 euro, nie przekraczającej 207 000 euro na dostawy materiałów opatrunkowych dla Wojewódzkiego Szpitala Specjalistycznego im. M. Kopernika w Łodzi.

ODPOWIEDZI NA ZAPYTANIA I MODYFIKACJA SPECYFIKACJI ISTOTNYCH WARUNKÓW ZAMÓWIENIA

Zgodnie z art. 38 ust. 2 ustawy z dnia 29 stycznia 2004r. prawo zamówień publicznych (tj. Dz. U z 2013 r. poz. 907) przekazujemy Państwu odpowiedzi na zapytania złożone do specyfikacji istotnych warunków zamówienia.

I. W toku postępowania zostały zadane następujące pytania i prośby o wyjaśnienia dotyczące treści Specyfikacji Istotnych Warunków Zamówienia:

Pytanie 1

Poz. 1 Czy można zaoferować pakiet do koronarografii o następującym składzie:
1. Prześcieradło angiograficzne – 1szt
- dwuwarstwowe, jałowe, wzmocnione
- rozmiar 320x290cm
- cztery otwory z przylepcem, umożliwiające nakłucie tętnicy promieniowej i udowej (lewa i prawa strona)
- przezroczysta folia z prawej i lewej strony wzdłuż prześcieradła
- środek wzmocniony, dodatkowa warstwa
2. Fartuchy operacyjne – 2 szt.
- jednorazowe, jałowe, wzmocnione
- rozmiar. „ L" – (130cm)
3. Serweta absorbcyjna rozm .- min. 40cm x 60 cm – 1 szt
4. Foliowy pokrowiec z gumką (na wzmacniacz) o rozm min. 100 x 100cm - 1 szt
5. Foliowy pokrowiec z gumką (osłona) o rozm. Min.60-90cm (gumka na krótszej krawędzi) - 1 szt
6. Foliowy pokrowiec z gumką (osłona) o rozm. Min.80-90cm (gumka na krótszej krawędzi) - 1 szt
7. Miska okrągła poj. 1litr, z przeznaczeniem do roztw. Heparyny – 1 szt
8. Ręczniki z włókniny kompresowej, wchłanialne – 2 szt
9. Kompresy gazowe rozmiar. 10x10 cm - 50 szt
10. Ostrze nr 11 bezpieczne zintegrowane z rączką – 1 szt
11. Strzykawka 20ml dokręcana – 1 szt
12. Strzykawka 20ml Luer –1 szt
13. Strzykawka 10ml Luer – 2 szt
14. Strzykawka 5ml Luer –1 szt
15. Szew chirurgiczny-nitka nie wchłanialna rozm 0 , z igłą trójkątną 3/8 c - 1 szt.
16. Serweta dwuwarstwowa – 1 szt.

Rozmiar min. 150x150cm – do przykrycia stolika zabiegowego, jednocześnie jest opakowaniem.

Odpowiedź:
Zamawiający podtrzymuje zapisy siwz

Pytanie 2
1. *Czy Zamawiający wyrazi zgodę na złożenie próbek dla Pakietu 1 w wersji niejałowej?*
2. *Czy Zamawiający wyrazi zgodę na złożenie próbki dla Pakietu 1 w ilości 1 szt.?*

Ad1 Odpowiedź:
Zamawiający dopuszcza w zakresie pakietu nr 1 złożenie próbek w wersji niejałowej

Ad 2 Odpowiedź
Zamawiający podtrzymuje zapisy siwz

pytania dotyczące umowy

1. *Zważywszy na treść § 1 ust. 4 wzoru umowy, jaką minimalną ilość (jaki procent ilości wskazanych w SIWZ) Zamawiający na pewno zamówi?*
Odpowiedź na powyższe pytanie ma istotne znaczenie dla odpowiedniej kalkulacji oferowanej ceny. Zgodnie z poglądem Krajowej Izby Odwoławczej wyrażonym m.in. w wyroku z dnia 18 czerwca 2010 r. KIO 1087/10, z art. 29 ust. 1 ustawy Prawo zamówień publicznych wynika obowiązek dokładnego określenia przez zamawiającego ilości zamawianych produktów; zamawiający nie jest zwolniony z tego obowiązku nawet jeżeli nie jest w stanie przewidzieć dokładnych ilości zamawianych produktów. W wyroku z dnia 7 maja 2014 r. KIO 809/14 Krajowa Izba Odwoławcza stwierdziła, że „nie można zaakceptować postanowień umowy dających zamawiającemu całkowitą, nieograniczoną pod względem ilościowym i pozostającą poza wszelką kontrolą dowolność w podjęciu decyzji o zmniejszeniu zakresu dostaw będących przedmiotem zamówienia".
2. *Czy Zamawiający odstąpi od wymogu umieszczania na fakturze numeru zamówienia? (§ 2 ust. 9 umowy)*
3. *Czy Zamawiający zgadza się aby w § 6 ust. 1 lit. b) wzoru umowy wyrażenie „10% wartości umowy brutto" zostało zastąpione wyrażeniem „10% niezrealizowanej wartości umowy brutto"?*
Uzasadnione jest aby kara umowna za odstąpienie od umowy była naliczana proporcjonalnie do wartości niezrealizowanej części umowy, nie zaś od wartości całej umowy. W przeciwnym razie, w przypadku odstąpienia od umowy po zrealizowaniu jej znaczącej części, kara umowna byłaby niewspółmiernie wysoka w stosunku do wartości niezrealizowanej części umowy, a nawet mogłaby przewyższać wartość niezrealizowanej

części umowy. Taka kara byłaby rażąco wygórowana w rozumieniu art. 484 § 2 Kodeksu cywilnego.

4. Czy Zamawiający zgadza się aby w § 6 ust. 1 lit. c), d) i e) wzoru umowy słowa „opóźnienie", „opóźnienia" zostały zastąpione odpowiednio słowami „zwłokę", „zwłoki"? Uzasadnione jest aby przesłanką naliczenia kary umownej była zwłoka (czyli opóźnienie zawinione przez wykonawcę), nie zaś za wszelkie opóźnienia, czyli także niezawinione przez wykonawcę. Nie ma uzasadnienia rozszerzanie odpowiedzialności wykonawcy także na niezawinione naruszenie terminu. Zgodnie z wyrokiem Krajowej Izby Odwoławczej z dnia 17 lipca 2014 r. KIO 1338/14; KIO 1377/14, „kara umowna należy się za niewykonanie lub nienależyte wykonanie umowy (art. 483 i nast. Kodeksu cywilnego), a więc tradycyjnie za zwłokę, a nie każde opóźnienie w wykonaniu umowy."

5. Czy Zamawiający zgadza się aby w § 8 ust. 2 wzoru umowy zostało dodane zdanie o następującej (lub podobnej) treści: „Przed rozwiązaniem umowy Zamawiający pisemnie wezwie Wykonawcę do należytego wykonywania umowy."?
Zważywszy na doniosłe i nieodwracalne skutki prawne rozwiązania umowy, celowe jest aby przed rozwiązaniem umowy Zamawiający wezwał wykonawcę do należytego wykonywania umowy. Takie wezwanie najprawdopodobniej zmobilizuje wykonawcę do należytego wykonywania umowy i pozwoli uniknąć rozwiązania umowy, a tym samym uniknąć skutków rozwiązania umowy, które są niekorzystne dla obu stron.

6. Jaka jest treść Polityki Bezpieczeństwa Informacji, o której mowa w § 10 ust. 3 i 4 wzoru umowy?
Jeżeli wykonawca ma się zobowiązać do przestrzegania Polityki Bezpieczeństwa Informacji, to musi znać jej treść.

7. Zważywszy, że § 11 ust. 1 wzoru umowy zawiera oświadczenie wykonawcy, iż jest mu znany stan majątkowy Zamawiającego, jaki jest aktualnie stan majątkowy Zamawiającego? Proszę o krótki opis. Czy Zamawiający zalega z płaceniem swoich zobowiązań?
Udzielając odpowiedzi na powyższe pytania proszę wziąć pod uwagę bieżące orzecznictwo Krajowej Izby Odwoławczej dotyczące umów.
Zgodnie z wyrokiem Krajowej Izby Odwoławczej z dnia 29 czerwca 2009 r. KIO/UZP 767/09, „mimo iż sytuacja Zamawiającego przy kształtowaniu treści umowy jest silniejsza, powinien on brać pod uwagę nie tylko swoje interesy, ale także interesy Wykonawcy i starać się ułożyć stosunek prawny tak, aby te interesy były jak najbardziej zrównoważone". Podobne stanowisko Krajowa Izba Odwoławcza zajęła w wyroku z dnia 21 lutego 2008 r. KIO/UZP 97/08, w wyroku z dnia 27 grudnia 2011 r. KIO 2649/11, w wyroku z dnia 17 grudnia 2012 r. KIO 2631/12, KIO 2655/12 oraz w wielu innych orzeczeniach.

Ad 1) Zamawiający podtrzymuje zapisy siwz. Zgodnie z § 1 pkt 4 „Zamawiający zastrzega sobie prawo niezrealizowania umowy w całości. Realizacja umowy uzależniona jest od faktycznej ilości pacjentów dla których leczenia niezbędny okaże się zakup towaru danego rodzaju."

Ad 2, 3, 4, 5, 8 Zamawiający podtrzymuje zapisy siwz.

WOJEWÓDZKI SZPITAL SPECJALISTYCZNY
im. M. Kopernika w Łodzi
Dział Zamówień Publicznych
tel. 042 689 5910, 5911, faks 042 689 54 04

Ad 6) Wyciąg z Polityki Bezpieczeństwa stanowi załącznik do niniejszego pisma.
Ad 7) Sytuacja majątkowa Zamawiającego wg stanu na dzień 31.08.2015 r.
Aktywa trwałe: 170 422 915,94 zł
Aktywa obrotowe: 66 281 384,73 zł
Suma pasywów: 236 704 300,67 zł
Zobowiązania i rezerwy: 304 590 488,75 zł
Zobowiązania krótkoterminowe: 108 216 773,94 zł
w tym wymagalne: 20 411 541,97 zł

Pozostałe postanowienia Specyfikacji Istotnych Warunków Zamówienia nie ulegają zmianie.

Z poważaniem

DYREKTOR
Wojewódzkiego Szpitala Specjalistycznego
im. M. Kopernika w Łodzi
(2)
mgr Wojciech Szrajber

1. Wstęp

Niniejszy dokument ma na celu sprecyzowanie wytycznych i zasad bezpieczeństwa, niezbędnych do poprawnego ustanowienia i funkcjonowania systemu zarządzania bezpieczeństwem informacji zgodnie z wymaganiami normy PN-ISO/IEC 27001:2007. Zapewnienie skutecznego i efektywnego systemu zarządzania bezpieczeństwem informacji ma na celu ochronę informacji adekwatnie do poziomu ryzyka, z wykorzystaniem najlepszych praktyk oraz przy pełnym uwzględnieniu uwarunkowań prawnych, organizacyjnych i technicznych.

Polityka Bezpieczeństwa Informacji jest dokumentem, który określa podstawowe cele Szpitala w obszarze bezpieczeństwa informacji (w tym danych osobowych) i przedstawia przyjęte podstawowe zasady postępowania i obowiązki pracowników Szpitala w zakresie bezpieczeństwa informacji i posiadanych aktywów.

Niniejszy dokument dotyczy:

1) ochrony istotnych informacji i zasobów posiadanych przez Szpital lub jego pracowników w wyniku wykonywanych czynności służbowych z wyłączeniem informacji niejawnych, których zakres, ochronę i przetwarzanie regulują odrębne przepisy prawa,
2) wytycznych do zapewnienia bezpieczeństwa fizycznego, teleinformatycznego i osobowego. Cele i zasady w zakresie bezpieczeństwa informacji są definiowane i uszczegóławiane w funkcjonujących dokumentach (regulaminy, procedury, instrukcje i plany).

Polityka Bezpieczeństwa Informacji oraz inne związane z nią dokumenty (w tym zapisy, będące dowodem wykonania określonych działań) z zakresu bezpieczeństwa informacji nazywane są łącznie dokumentacją bezpieczeństwa informacji.

Struktura dokumentacji bezpieczeństwa informacji przedstawiona jest w dalszej części niniejszego dokumentu.

Użyte w niniejszej polityce sformułowania takie jak: **„obowiązkowe jest"**, **„wymagane jest"**, **„należy"**, **„musi"**, **„powinno być"** oznaczają wymóg stosowania.

Sformułowania takie jak: **„zakazane jest", „nie może"** oznaczają zakaz stosowania, opisanego w dalszej części.

Użyte w niniejszej Polityce sformułowania takie jak **„zalecane jest"** oznaczają, że odstąpienie przez pracownika od opisanego w dalszej części trybu postępowania jest dozwolone, jeżeli uzasadniają to okoliczności. Przy braku okoliczności uzasadniających odstąpienie, należy stosować postępowanie takie, jak opisano w tym sformułowaniu.

Sformułowania takie jak **„dopuszczalne jest", „dopuszcza się", „może"** oznaczają, że odstąpienie od opisanego
w dalszej części trybu postępowania leży w gestii pracownika i nie wymaga uzasadnienia.

Sformułowanie **„niezwłocznie"** oznacza konieczność realizacji zadania tak szybko jak jest to możliwe.

1.1 Zakres obowiązywania dokumentu

Zakres obowiązywania niniejszej Polityki dotyczy:

- ✓ określenia własności aktywów i zasad postępowania z nimi, w szczególności wyposażenia, systemów, urządzeń przetwarzających informacje w dowolnej formie: elektronicznej, papierowej, utrwalonej na slajdach, kliszach itp.,
- ✓ zasad udostępniania dokumentacji bezpieczeństwa informacji, o których decyduje Pełnomocnik ds. Bezpieczeństwa lub Kierownik Pionu organizacji i systemów Zarządzania. O zakresie udostępnienia tej dokumentacji konkretnemu pracownikowi decyduje, z zachowaniem wyżej wymienionych zasad oraz zasady wiedzy niezbędnej, bezpośredni przełożony pracownika,
- ✓ określenia stref bezpieczeństwa fizycznego oraz zasad w nich panujących,
- ✓ zapewnienia ciągłości działania Szpitala.

Nieprzestrzeganie postanowień zawartych w dokumentacji bezpieczeństwa informacji może skutkować sankcjami w pełnym zakresie dopuszczonymi przez stosunek pracy (zawartą umowę) pomiędzy Szpitalem a pracownikiem (lub podmiotem) oraz obowiązujące przepisy prawa. W przypadku informacji i systemów teleinformatycznych zawierających dane osobowe, pierwszeństwo mają przepisy z zakresu ochrony danych osobowych.

1.2 Adresaci dokumentu

Niniejsza Polityka obowiązuje wszystkich pracowników Szpitala oraz podmioty współpracujące ze Szpitalem rozumianych jako Adresaci dokumentu. Każdy z pracowników Szpitala oraz podmiot świadczący usługi dla Szpitala związane z przetwarzaniem danych osobowych, ma obowiązek zapoznać się z tą dokumentacją we właściwym dla niego zakresie i przestrzegać zawartych w niej postanowień (Polityka Bezpieczeństwa Informacji, Regulamin użytkownika systemu informatycznego oraz procedur postępowania w przypadkach naruszenia bezpieczeństwa i pozostałe procedury systemowe).

1.3 Dokumenty powołane

Zidentyfikowano wymagania dotyczące bezpieczeństwa informacji przetwarzanych w Szpitalu oraz przyporządkowano te wymagania do odpowiednich punktów załącznika A normy PN-ISO/IEC 27001:2007 dotyczącej tworzenia systemu zarządzania bezpieczeństwem informacji.

Przy opracowaniu niniejszej Polityki uwzględnione zostały przepisy właściwych aktów prawnych. Ich wykaz dostępny jest na stronie wewnętrznej Szpitala.

1.4 Analiza uwarunkowań i ograniczeń

Tam, gdzie ustawodawca przewidział szczególne sankcje za naruszenie wymagań normy prawnej, zostały one wskazane przy opisie konkretnego wymagania. W przeciwnym przypadku należy uznać, iż ewentualna odpowiedzialność za naruszenie przepisu oparta jest o ogólne zasady odpowiedzialności w konkretnym obszarze działalności.

1.5 Słownik pojęć

Dla potrzeb niniejszej Polityki definiuje się następujące pojęcia:

Szpital	Wojewódzki Szpital Specjalistyczny im. M. Kopernika w Łodzi
Administrator Danych Osobowych (ADO)	Dyrektor Szpitala
użytkownik/pracownik	- osoba zatrudniona w Szpitalu, która podczas wykonywanych obowiązków może przetwarzać dane, posiadająca stosowne upoważnienie do przetwarzania danych osobowych , - osoba przetwarzająca dane w toku wykonywania umowy cywilno-prawnej (umowa zlecenia, o dzieło, kontrakt itp.), - pracownik innego podmiotu zewnętrznego, który świadczy usługi na rzecz Szpitala, na podstawie odrębnej umowy z tym podmiotem (np. serwis, zlecenie, przetwarzanie danych, usługa, dostawa itp.)
aktywa	wszystko, co stanowi wartość dla Szpitala (np. zasoby ludzkie, wartość materialna: komputery, bazy danych itp.; wartość niematerialna: dobre imię, itp.); na potrzeby niniejszej Polityki aktywa dzielone są na informacje (np. dokumenty) oraz zasoby (np. pracownicy, wyposażenie)
właściciel aktywa - gestor	kierownik komórki organizacyjnej Szpitala odpowiedzialny za aktywa oraz za określenie zasad dostępu i jego użycia
zasoby	dowolny element systemu przetwarzania danych potrzebny do operacji (np. urządzenia pamięciowe, jednostki centralne, dane, pliki, programy, itp.)
nośniki danych	przedmiot fizyczny, na którym możliwe jest zapisanie informacji, i z którego możliwe jest jej późniejsze odczytanie (np. papier, taśma, klisza, dyskietka, dysk HDD, płyta CD DVD, karta pamięci, pamięć USB, kardridż, kaseta video, itp.)
hasło	ciąg znaków literowych, cyfrowych, lub innych znany jedynie osobie uprawnionej, umożliwiający korzystanie z systemu
identyfikator użytkownika	ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną
dane osobowe	wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, przetwarzane zarówno w systemach informatycznych jak i tradycyjnie (wersja papierowa). osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne. Informacji nie uważa się za umożliwiające określenie tożsamości osoby tylko wówczas, gdy wymagałoby to nadmiernych kosztów, czasu lub działań
dane osobowe wrażliwe	szczególne dane osobowe np. dane o stanie zdrowia, kodzie genetycznym, przekonaniach filozoficznych czy religijnych
przetwarzanie danych osobowych	jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie danych osobowych, w szczególności w systemach informatycznych

obszar przetwarzania danych	Infrastruktura, obiekt, pomieszczenie Szpitala, w którym odbywa się przetwarzanie danych
obszar bezpieczny	wydzielona i zabezpieczona powierzchnia, gdzie jest zapewniona ochrona fizyczna przetwarzanych informacji. Obszarem bezpiecznym może być np. serwerownia
dostępność	właściwość bycia dostępnym i użytecznym na żądanie upoważnionego podmiotu
integralność	właściwość polegająca na zapewnieniu dokładności i kompletności aktywów
poufność	właściwość polegająca na tym, że informacja nie jest udostępniana lub wyjawiana nieupoważnionym osobom, podmiotom lub procesom
autentyczność	właściwość zapewniająca, że tożsamość podmiotu lub procesu jest taka, jak deklarowana
rozliczalność	właściwość zapewniająca możliwość przypisania określonego działania w systemie teleinformatycznym konkretnemu użytkownikowi
uwierzytelnienie	uwiarygodnienie swojej tożsamości względem systemu teleinformatycznego
analiza ryzyka	systematyczne wykorzystanie informacji do zidentyfikowania źródeł i oszacowania ryzyka
szacowanie ryzyka	całościowy proces analizy i oceny ryzyka
ocena ryzyka	proces porównania ryzyka z określonymi kryteriami w celu określenia znaczenia ryzyka
audyt	działania mające na celu ocenę danej osoby, Szpitala, systemu, procesu, zabezpieczenia mające na celu potwierdzenie spełnienia konkretnych wymagań
niezgodność	stan systemu lub zabezpieczenia inny niż zdefiniowany w wymaganiach i standardach wewnętrznych i zewnętrznych
działania korygujące	działania podejmowane w celu eliminacji przyczyny niezgodności w celu zapobiegania ich powtórnemu wystąpieniu
działania zapobiegawcze	działania podejmowane w celu eliminacji przyczyny potencjalnych niezgodności w celu zapobiegania ich wystąpienia
zdarzenie	określony stan systemu, usługi lub sieci, który wskazuje na możliwe naruszenie polityki bezpieczeństwa informacji, błąd zabezpieczenia lub nieznaną dotychczas sytuację, która może być związana z bezpieczeństwem informacji
incydent bezpieczeństwa informacji	pojedyncze zdarzenie lub seria niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, które stwarzają znaczne prawdopodobieństwo zakłócenia działań biznesowych i zagrażają bezpieczeństwu informacji
zabezpieczenie	środki służące zarządzaniu ryzykiem, łącznie z politykami, procedurami, zaleceniami, praktyką lub strukturami organizacyjnymi, które mogą mieć naturę administracyjną, techniczną, zarządczą lub prawną
zagrożenie	potencjalna przyczyna niepożądanego incydentu, który może wywołać szkodę w Szpitalu
deklaracja stosowania	dokument, w którym opisano cele stosowania zabezpieczeń, które odnoszą się i mają zastosowanie w SZBI
bezpieczeństwo informacji	zachowanie poufności, integralności i dostępności informacji; dodatkowo, mogą być brane pod uwagę inne własności, takie jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność
bezpieczeństwo fizyczne	zespół rozwiązań organizacyjnych i materialnych przeciwdziałających zagrożeniom związanym z nieuprawnionym dostępem do zasobów fizycznych, szkodliwymi czynnikami środowiskowymi oraz zakłóceniami zasilania, które mogą negatywnie wpływać na działanie Szpitala
System Zarządzania Bezpieczeństwem Informacji (SZBI)	część całościowego systemu zarządzania, oparta na podejściu wynikającym z ryzyka biznesowego, odnosząca się do ustanawiania, wdrażania, eksploatacji, monitorowania, utrzymywania i doskonalenia bezpieczeństwa informacji

Zintegrowany System Zarządzania Jakością i Zarządzania Bezpieczeństwem Informacji (ZSZJiZBI)	system zarządzania spełniający wymagania podstawowych elementów systemów oraz możliwości takiego ich kształtowania, aby spełniały jednocześnie kryteria funkcjonowania Szpitala oraz wymagania zawarte w normach ISO serii 9000, ISO serii 27000
Administrator Bezpieczeństwa Teleinformatycznego (ABT)	osoba odpowiedzialna za zarządzanie obszarem bezpieczeństwa teleinformatycznego w Szpitalu
Administrator Bezpieczeństwa Fizycznego i Osobowego (ABFiO)	osoba odpowiedzialna za zarządzanie obszarem bezpieczeństwa fizycznego i osobowego w Szpitalu. Pełni obowiązki Administratora Bezpieczeństwa Informacji
Administrator Systemu (AS)	osoba zarządzająca bieżącą pracą systemu informatycznego i zbiorami danych w Szpitalu
Administrator urządzenia	osoba odpowiedzialna za zarządzanie, konfigurację i konserwację urządzenia
Pełnomocnik ds. Bezpieczeństwa (PB)	osoba odpowiedzialna za funkcjonowanie systemu zarządzania bezpieczeństwem informacji w Szpitalu

1.6 Nienaruszalne zasady bezpieczeństwa

System zarządzania bezpieczeństwem informacji zgodny z wymaganiami niniejszej Polityki opiera się na następujących niezaprzeczalnych zasadach ochrony informacji:

- ✓ **Zasada znajomości wymagań polityki bezpieczeństwa informacji.** Każdy pracownik musi zostać zapoznany z regułami oraz z kompletnymi i aktualnymi procedurami ochrony informacji obowiązujących w jego komórce organizacyjnej i podpisać stosowne oświadczenie o zapoznaniu się z zasadami obowiązującej Polityki;
- ✓ **Zasada uprawnionego dostępu.** Każdy pracownik stosuje się do obowiązujących zasad ochrony informacji i spełnia kryteria dopuszczenia do informacji;
- ✓ **Zasada przywilejów koniecznych.** Każdy pracownik posiada prawa dostępu do informacji, ograniczone wyłącznie do tych, które są konieczne do wykonywania powierzonych mu zadań;
- ✓ **Zasada wiedzy koniecznej.** Każdy pracownik posiada wiedzę o systemie do którego ma dostęp, ograniczoną wyłącznie do zagadnień, które są konieczne do realizacji powierzonych mu zadań;
- ✓ **Zasada usług koniecznych**. Systemy informacyjne świadczą tylko takie usługi, które są konieczne do realizacji zadań biznesowych i operacyjnych;
- ✓ **Zasada asekuracji.** Każdy mechanizm zabezpieczający musi być ubezpieczony drugim (podobnym). W przypadkach szczególnych może być stosowane dodatkowe (trzecie) niezależne zabezpieczenie. Jako mechanizmy zabezpieczeń dopuszczalne jest stosowanie zabezpieczeń technicznych jak i organizacyjnych;
- ✓ **Zasada wyłączności.** Za konfigurowanie systemów bezpieczeństwa informacji nie może być odpowiedzialna osoba, która jednocześnie odpowiedzialna jest za kontrolę ich funkcjonowania;
- ✓ **Zasada świadomości zbiorowej.** Wszyscy pracownicy są świadomi konieczności ochrony zasobów informacyjnych i aktywnie uczestniczą w tym procesie;
- ✓ **Zasada indywidualnej odpowiedzialności.** Za bezpieczeństwo poszczególnych elementów odpowiadają poszczególne osoby;
- ✓ **Zasada obecności koniecznej.** Prawo przebywania w określonych miejscach mają tylko osoby do tego upoważnione;
- ✓ **Zasada stałej gotowości.** System jest zabezpieczony na wypadek wystąpienia zagrożeń. Niedopuszczalne jest tymczasowe wyłączanie mechanizmów zabezpieczających;
- ✓ **Zasada najsłabszego ogniwa.** Poziom bezpieczeństwa wyznacza najsłabszy (najmniej zabezpieczony) element. Elementy takie są wyznaczane w oparciu o wyniki analizy ryzyka;
- ✓ **Zasada kompletności.** Skuteczne zabezpieczenie jest tylko wtedy, gdy stosuje się podejście kompleksowe, uwzględniające wszystkie stopnie i ogniwa ogólnie pojętego procesu przetwarzania informacji;
- ✓ **Zasada ewolucji.** Każdy system musi ciągle dostosowywać mechanizmy wewnętrzne do zmieniających się warunków zewnętrznych;
- ✓ **Zasada odpowiedniości.** Używane mechanizmy muszą być adekwatne do sytuacji;
- ✓ **Zasada akceptowanej równowagi.** Podejmowane środki zaradcze nie mogą przekraczać poziomu akceptacji;
- ✓ **Zasada świadomej konwersacji. Nie zawsze i wszędzie trzeba mówić, co się wie, ale zawsze i wszędzie trzeba wiedzieć co, gdzie i do kogo się mówi.**

1.7 Dokumentacja bezpieczeństwa informacji

Dokumentacja systemu zarządzania bezpieczeństwem informacji w Szpitalu obejmuje w szczególności:

- ✓ Księgę Zintegrowanego Systemu Zarządzania,
- ✓ Politykę Zintegrowanego Systemu Zarządzania Jakością i Zarządzania Bezpieczeństwem Informacji,

- ✓ Ogólna i Szczegółową Politykę Bezpieczeństwa Informacji
- ✓ Deklarację stosowania,
- ✓ Instrukcję zarządzania systemem informatycznym przetwarzającym dane osobowe,
- ✓ Regulamin użytkownika systemów informatycznych,
- ✓ szczegółowe procedury i instrukcje systemu zarządzania bezpieczeństwem informacji, ich wykaz zamieszczono w Załączniku nr 2 do niniejszego dokumentu,
- ✓ cele i zadania w systemie zarządzania bezpieczeństwem informacji,
- ✓ wewnętrzne akty normatywne niezbędne do zapewnienia planowania, realizacji i nadzorowania działalności w obszarze bezpieczeństwa informacji np. zarządzenia, regulaminy, itp.,
- ✓ zapisy w systemie zarządzania bezpieczeństwem informacji.

1.8 Podstawa prawna dokumentu

Niniejsza Polityka Bezpieczeństwa Informacji została zatwierdzona do stosowania w Szpitalu przez Dyrektora stosownym zarządzeniem.