KOPERNIK

WOJEWÓDZKI SZPITAL SPECJALISTYCZNY
im. M. Kopernika w Łodzi
ul. Pabianicka 62
93-513 Łódź

EZ/263/142/1301/2013

Łódź, dnia 26.09.2013r
Nr sprawy 142/ZP/13

Dotyczy: postępowania o udzielenie zamówienia publicznego prowadzonego w trybie przetargu nieograniczonego o wartości powyżej 14 000 euro, nie przekraczającej kwoty 200 000 euro na dostawę kateterów oskrzelowych dla Wojewódzkiego Szpitala Specjalistycznego im. M. Kopernika w Łodzi.

ODPOWIEDZI NA PYTANIA ORAZ ZMIANA SPECYFIKACJI ISTOTNYCH WARUNKÓW ZAMÓWIENIA

Zgodnie z art. 38 ustawy z dnia 29 stycznia 2004r. Prawo zamówień publicznych (tj. Dz. U. z 2013r poz. 907 ze zm.) przekazujemy Państwu odpowiedzi na pytania i zmianę Specyfikacji Istotnych Warunków Zamówienia w postępowaniu na dostawy kateterów oskrzelowych dla Wojewódzkiego Szpitala Specjalistycznego im. M. Kopernika w Łodzi.

1. W toku prowadzonego postępowania zostały zadane następujące pytania:

1. SIWZ Załącznik nr 3 do SIWZ, "Wzór umowy" § 1 ust. 5
Prosimy o dodanie do ustępu 5 po kropce zdania: Dostawa potwierdzona będzie protokołem dostawy.
Odpowiedź: Zamawiający wyraża zgodę

2. SIWZ Załącznik nr 3 do SIWZ, "Wzór umowy" § 1 ust. 12
Czy Zamawiający wyrazi zgodę na zmianę treści na:
„W przypadku stwierdzenia wad fizycznych lub braków ilościowych w dostarczonym towarze Zamawiający niezwłocznie w terminie nie dłuższym niż 3 dni od doręczenia dostawy zawiadomi i tym Wykonawcę oraz opisze wady lub braki w protokole dostawy. Wykonawca bezzwłocznie wymieni wadliwy towar na wolny od wad lub dostarczy brakujący towar zgodnie z zamówieniem (co do rodzaju, jakości i ilości)- w terminie nie dłuższym niż 7 dni roboczych od głoszenia danej reklamacji. W przypadku braku informacji o wadach lub brakach w wyżej wskazanym terminie, dostawę uznaję się jako wykonaną należycie. „

Odpowiedź: Zamawiający zmienia zapisy SIWZ

3. SIWZ Załącznik nr 3 do SIWZ, "Wzór umowy" § 1
W związku z faktem, iż przedmiot umowy produkowany jest tylko przez jednego producenta prosimy o wykreślenie ustępu 14 lub dodanie do § 1 ustępu o następującym brzmieniu:

KOPERNIK

WOJEWÓDZKI SZPITAL SPECJALISTYCZNY
im. M. Kopernika w Łodzi
ul. Pabianicka 62
93-513 Łódź

„ Zamawiający dokonuje zakupu u podmiotu trzeciego na własna odpowiedzialność i musi dopełnić wszelkiej staranności w celu potwierdzenia kompatybilności z urządzeniem w jakim będzie wykorzystywane."
Odpowiedź: Zamawiający wyraża zgodę

4. SIWZ Załącznik nr 3 do SIWZ, "Wzór umowy" § 2 ust. 1
Czy w związku z faktem, że przedmiotem zamówienia jest dostawa wyrobów medycznych, za które odpowiedzialność ponosi wytwórca i on jest audytowany przez jednostkę notyfikowaną, której certyfikat potwierdza spełnienie wymagań zasadniczych oraz możliwość sprzedaży i stosowania w celach medycznych w związku z czym audyt u dostawcy jest bezcelowy, Zamawiający wyrazi zgodę na wykreślenie ustępu 1 w całości?
Odpowiedź: Zamawiający podtrzymuje zapisy SIWZ. : Audit dostawcy (audit pozaplanowy) przeprowadzany jest w sytuacjach wymagających zwiększenia nadzoru nad dostawcą, wówczas, gdy jest to uzasadnione, np., wizerunek firmy dostawcy niekorzystnie wpływa na funkcjonowanie i jakość usług Szpitala, świadczenie usług odbywa się z narażeniem warunków umowy lub gdy zaistnieją takie podejrzenia

5. SIWZ Załącznik nr 3 do SIWZ, "Wzór umowy" § 2 ust. 2
Czy Zamawiający wyrazi zgodę na zmianę treści ustępu na: „Wszelkie informacje, uzyskane przez strony umowy w związku z realizacją niniejszej umowy, zarówno Zamawiający jak i Wykonawca powinni traktować jako poufne w trakcie obowiązywania umowy oraz po jej zakończeniu."?
Odpowiedź: Zamawiający podtrzymuje zapisy SIWZ. Zamawiający jako jednostka finansów publicznych zobowiązany jest zasadą jawności wydatkowania środków publicznych oraz transparentnością zawieranych umów i ich realizacji. Dlatego też nie może przyjąć na siebie zasady obowiązku poufności. Z kolei obowiązek poufności po stronie Wykonawcy dotyczy przede wszystkim ochrony wrażliwych danych osobowych pacjentów Szpitala, z którymi Wykonawca może się zetknąć.

6. SIWZ Załącznik nr 3 do SIWZ, "Wzór umowy" § 2 ust. 3,4.
Zamawiający proszony jest o przedstawienie „Polityki Bezpieczeństwa Informacji" lub wykreślenie ustępów 3 i 4 w całości?
Odpowiedź: Zamawiający przedstawia w załączeniu wyciąg z polityki bezpieczeństwa

7. SIWZ Załącznik nr 3 do SIWZ, "Wzór umowy" § 3 ust. 6
W związku z brakiem możliwości zamieszczenia na fakturze daty ważności i numeru serii dostarczonego towaru prosimy o zmianę ustępu 6 na następujący:

ul. Pabianicka 62, 93-513 Łódź, SEKRETARIAT tel. (42) 689 50 10/fax (42) 689 50 11;
CENTRALA tel. (42) 689 50 00,e-mail: szpital@kopernik.lodz.pl, http://www.kopernik.lodz.pl
NIP 729-23-45-599 REGON 000295403 PEKAO S.A. O/ŁÓDŹ 62124015451111000011669957

„Faktura oraz inny dokument potwierdzający dostawę winny bezwzględnie obejmować sprzęt medyczny tylko z niniejszej umowy i zawierać wskazanie numeru niniejszej umowy oraz numeru zamówienia (zamówień)~~, daty ważności oraz numeru serii dostarczonego produktu~~ w związku z którymi nastąpiła dostawa."
Odpowiedź: Zamawiający wyraża zgodę.

8. SIWZ Załącznik nr 3 do SIWZ, "Wzór umowy" § 4 ust. 1
W związku z tym, iż Wykonawca jest w stałym kontakcie z producentem w związku z czym o wprowadzeniu nowego lub udoskonalonego wyrobu będzie posiadał informacje w pierwszej kolejności proponujemy zastrzeżenie zmian w umowie wynikających z ust. 1 § 4 zamienić na następujące:
„1) wprowadzenia wyrobu medycznego nowego lub udoskonalonego, spełniającego parametry wymagane w SIWZ, pod warunkiem zachowania ceny jednostkowej netto na poziomie nie wyższym, niż wyrób objęty zamówieniem początkowym. Ewentualna zmiana wyrobu może być dokonana na pisemny wniosek Wykonawcy, poprzez zawarcie aneksu, w którym dotychczasowy wyrób zostanie wykreślony i zastąpiony wyrobem zmodyfikowanym lub udoskonalonym"
Odpowiedź: Zamawiający podtrzymuje zapisy SIWZ. W umowie prawo występowania z wnioskiem o zmianę ma każda ze stron, zaś taka zmiana wymaga i tak wyrażenia zgody obu stron.

9. SIWZ Załącznik nr 3 do SIWZ, "Wzór umowy" § 4 ust. 2
W związku z tym, iż przedmiot umowy produkowany jest przez jednego producenta w przypadku jego wycofania nie jest możliwe zapewnienie wyrobu zamiennego jeśli producent go nie zapewni, a wiec całkiem niezależnie od Wykonawcy proponujemy zastrzeżenie zmian w umowie wynikających z ust. 2 § 4 zamienić na następujące:
„2) wycofania wyrobu medycznego z produkcji – ~~Wykonawca ma obowiązek zapewnić dostarczenie wyrobu zamiennego o parametrach nie gorszych od produktu objętego umową pod warunkiem zachowania ceny jednostkowej netto na poziomie nie wyższym, niż wyrób objęty zamówieniem początkowym.~~ Ewentualna zmiana wyrobu może być dokonana na pisemny wniosek Wykonawcy, poprzez zawarcie aneksu, mocą którego nastąpi wykreślenie z umowy wyrobu wycofanego z produkcji lub zastąpienie go wyrobem zamiennym o ile producent taki zapewni."
Odpowiedź: Zamawiający podtrzymuje zapisy SIWZ

10. SIWZ Załącznik nr 3 do SIWZ, "Wzór umowy" § 4 ust. 4
W celu zapewnienia równości stron umowy proponujemy zastrzeżenie zmian w umowie wynikających z ust. 4 § 4 zamienić na następujący:
„4) obniżenia stawki podatku VAT przy czym zmianie ulega jedynie cena brutto, cena netto pozostaje bez zmian. Nowe stawki będą obowiązywać strony wraz z wejściem w życie przepisów je regulujących. Każdorazowa zmiana nie wymaga sporządzenia aneksu w formie pisemnej, ewentualnie strony mogą zawrzeć aneks porządkujący na wniosek Zamawiającego. W uzasadnionych wypadkach, na

ul. Pabianicka 62, 93-513 Łódź, SEKRETARIAT tel. (42) 689 50 10/fax (42) 689 50 11;
CENTRALA tel. (42) 689 50 00,e-mail: szpital@kopernik.lodz.pl, http://www.kopernik.lodz.pl
NIP 729-23-45-599 REGON 000295403 PEKAO S.A. O/ŁÓDŹ 62124015451111000011669957

pisemny umotywowany wniosek Wykonawcy strony mogą zawrzeć aneks, mocą którego zdecydują o podwyższeniu ceny netto przy pozostawieniu ceny brutto bez zmian; w takiej sytuacji strony mogą zdecydować również o odpowiednim do spadku stawki podatku VAT podwyższeniu wartości netto w całej umowy ze skutkiem od dnia określonego w treści aneksu. "

Odpowiedź: Zamawiający podtrzymuje zapisy SIWZ. Umowa jest na 6 miesięcy, nie jest planowane w tym czasie obniżenie stawek podatku VAT.

11. SIWZ Załącznik nr 3 do SIWZ, "Wzór umowy" § 4 ust. 6

W związku z tym, iż przedmiot umowy produkowany jest tylko przez jednego producenta w przypadku przejściowego braku wyrobu z przyczyn leżących po stronie producenta niemożliwe będzie zapewnienie produktu zastępczego, prosimy o wykreślenie ustępu 6 § 4 w całości.

Odpowiedź: Zamawiający wyraża zgodę na wykreślenie ale zaznacza, że Wykonawca zobowiązany jest do zabezpieczenia takiej ilości wyrobów medycznych w swoich magazynach, aby realizacja całej umowy w całym jej okresie możliwa była do maksymalnej szacunkowej ilości zamawianych wyrobów (która wynosi 60sztuk)

12. SIWZ Załącznik nr 3 do SIWZ, "Wzór umowy" § 5 ust. 1

Czy Zamawiający wyrazi zgodę na wykreślenie wyrazu „organizacyjnych" w każdej osobie i formie oraz wykreślenie treści w brzmieniu „ i zmianie adresu zamieszkania właściciela lub współwłaściciela firmy" lub wyłączyć ją w stosunku do Wykonawców prowadzących działalność w formie spółki z ograniczoną odpowiedzialnością?

Odpowiedź: Zamawiający podtrzymuje zapisy SIWZ. Zapisy te oczywiście należy interpretować odpowiednio do formy prawnej w jakiej będzie działać Wykonawca

13. SIWZ Załącznik nr 3 do SIWZ, "Wzór umowy" § 7 ust. 1 lit. a) i b).

Czy Zamawiający wyrazi zgodę na zmianę wysokości kar umownych z 2 % na 0,2%? Pozostała treść bez zmian.

Odpowiedź: Zamawiający wyraża zgodę

14. SIWZ Załącznik nr 3 do SIWZ, "Wzór umowy" § 7 ust. 1 lit. d).

W związku z tym, iż przedmiot umowy jak i certyfikaty jego dotyczące były już dostarczane Zamawiającemu prosimy o całkowite wykreślenie zapisu lit. d ust. 1 § 7.

Odpowiedź: Zamawiający podtrzymuje zapisy SIWZ. Zamawiający wymaga złożenia dokumentów wymienionych w § 1 ust. 8 celu potwierdzenia, że oferowany sprzęt spełnia wymogi określone w przepisach prawnych.

15. SIWZ Załącznik nr 3 do SIWZ, "Wzór umowy" § 8

Czy w celu zachowania równości stron umowy Zamawiający wyrazi zgodę na dodanie do § 8 zapisów: „Wykonawcy przysługuje prawo rozwiązania umowy z zachowaniem 7 dniowego okresu wypowiedzenia w następujących sytuacjach :

ul. Pabianicka 62, 93-513 Łódź, SEKRETARIAT tel. (42) 689 50 10/fax (42) 689 50 11;
CENTRALA tel. (42) 689 50 00,e-mail: szpital@kopernik.lodz.pl, http://www.kopernik.lodz.pl
NIP 729-23-45-599 REGON 000295403 PEKAO S.A. O/ŁÓDŹ 62124015451111000011669957

a) opóźnienia Zamawiającego z jakąkolwiek płatnością przekraczającego 30 dni,
b) innego niewywiązywania się przez Zamawiającego z obowiązków nałożonych na niego niniejszą umową. Okres wypowiedzenia liczy się od dnia doręczenia Zamawiającemu pisemnego oświadczenia o rozwiązani umowy."
oraz dodanie zapisu w brzmieniu: „Wykonawcy przysługuje prawo odstąpienia od umowy w przypadku zalegania przez Zamawiającego z jakąkolwiek płatnością z tytułu niniejszej umowy. Oświadczenie o odstąpieniu od umowy zostanie złożone Zamawiającemu w terminie 60 dni od dnia powstania każdej z zaległości".
Odpowiedź: Zamawiający nie wyraża zgody, ze względu na szczególny charakter prowadzonej przez siebie działalności (działalność lecznicza) i istotne znaczenie przedmiotu zamówienia dla planowania leczenia pacjentów onkologicznych

16. SIWZ Załącznik nr 3 do SIWZ, "Wzór umowy" § 9 ust. 2
Czy Zamawiający wyrazi zgodę na wykreślenie zdania: „Strony wyłączają jednak między sobą zastosowanie art. 552 KC"?
Zamawiający nie wyraża zgody, ze względu na szczególny charakter prowadzonej przez siebie działalności (działalność lecznicza) i istotne znaczenie przedmiotu zamówienia dla planowania leczenia pacjentów onkologicznych

W załączeniu zmieniony Załącznik nr 3 do SIWZ – wzór umowy.

2. Zamawiający zmienia następujące terminy:
   - termin składania ofert do dnia 1 października 2013r. do godz. 10:00
   - termin otwarcia ofert w dniu 1 października 2013r. o godz. 11:00

Pozostałe postanowienia Specyfikacji Istotnych Warunków Zamówienia pozostają bez zmian.

p.o. ZASTĘPCA DYREKTORA
ds. [illegible]
dr n. prac. [illegible]

ul. Pabianicka 62, 93-513 Łódź, SEKRETARIAT tel. (42) 689 50 10/fax (42) 689 50 11;
CENTRALA tel. (42) 689 50 00,e-mail: szpital@kopernik.lodz.pl, http://www.kopernik.lodz.pl
NIP 729-23-45-599 REGON 000295403 PEKAO S.A. O/ŁÓDŹ 62124015451111000011669957

UMOWA NR ...../ZP/13 *wzór umowy – po zmianach*
z dnia _____

zawarta przez:
Wojewódzki Szpital Specjalistyczny im. M. Kopernika w Łodzi
wpisany do Krajowego Rejestru Sądowego Rejestru Stowarzyszeń, innych organizacji społecznych i zawodowych, fundacji i publicznych zakładów opieki zdrowotnej w Sądzie Rejonowym dla Łodzi – Śródmieścia w Łodzi, XX Wydział KRS pod numerem **0000004955** , REGON 000295403, NIP 729 - 23 - 45 - 599)
z siedzibą w Łodzi, ul. Pabianicka 62
reprezentowany przez .....
zwany dalej **Zamawiającym**
z
firmą .....
(REGON ..... NIP .....)
z siedzibą w ....., ulica .....,
wpisaną do ..... pod numerem .....
reprezentowaną przez.....,

zwaną dalej **Wykonawcą**

wyłonioną w wyniku postępowania o udzielenie zamówienia publicznego prowadzonego w trybie przetargu nieograniczonego na podstawie art. 39 w związku z art. 10 ust. 1 Ustawy Prawo Zamówień Publicznych z dnia 29.01.2004r.(tj. Dz. U. 2010r. nr 113 poz. 759 z późn. zm.) **na dostawy kateterów oskrzelowych dla Wojewódzkiego Szpitala Specjalistycznego im. M. Kopernika w Łodzi** obowiązującą od dnia _____ do dnia _____ o łącznej wartości ..... zł brutto (słownie: .....)

§1

1. Przedmiotem umowy jest sprzedaż wraz z dostawą wyrobów medycznych wyszczególnionych asortymentowo i cenowo w załączniku nr 1 do umowy, zwanych dalej również „towarem" lub „wyrobem".
2. Realizacja przedmiotu zamówienia będzie następowała sukcesywnie w okresie, na który została zawarta umowa zgodnie z bieżącym zapotrzebowaniem Zamawiającego, który będzie składał do Wykonawcy zamówienia częściowe.
3. Zamówienie towarów wyszczególnionych w załączniku nr 1 będzie zawierało zestawienie ilościowe i rodzajowe przedmiotowego towaru uzależnione od bieżącego zapotrzebowania Zamawiającego.
4. Zamówienia należy składać na nr faksu .....
5. Wykonawca będzie dostarczał towar fabrycznie nowy, wolny od wad fizycznych i prawnych do magazynu sprzętu medycznego Apteki Szpitalnej (nr tel. 42 689–51–08) Wojewódzkiego Szpitala Specjalistycznego im. M. Kopernika w Łodzi przy ul. Pabianickiej 62, oryginalnie zapakowany, w terminie do 3 tygodni od dnia otrzymania danego zamówienia. **Dostawa potwierdzona będzie protokołem dostawy**
6. Wykonawca dostarczy zamówiony towar na własny koszt i ryzyko w godzinach od 9.00 do 13.00
7. Wykonawca oświadcza, że dostarczane Zamawiającemu, w ramach niniejszej umowy, wyroby medyczne będą przez cały okres jej obowiązywania spełniać normy jakościowe oraz parametry użytkowe zgodne z opisem przedmiotu zamówienia określonym w SIWZ oraz treścią złożonej przez niego oferty przetargowej, jak również posiadać wszystkie bez wyjątku wymagane prawem dopuszczenia (rejestracje) do obrotu i użytkowania na terytorium RP.
8. Wykonawca, pod rygorem prawa Zamawiającego do jednostronnego wypowiedzenia niniejszej umowy z winy Wykonawcy, zobowiązany jest wraz z pierwszą dostawą towaru dostarczyć Zamawiającemu komplet aktualnych dokumentów (oryginał lub poświadczona za zgodność z oryginałem kopia) dopuszczających do obrotu

i użytkowania na terytorium RP wyroby medyczne, których dostawa stanowi przedmiot niniejszej umowy.

9. Wykonawca, bez wezwania, przy każdorazowej zmianie stanu prawnego związanego z dopuszczeniem do obrotu jak i użytkowania na terytorium RP, dostarczanych przez niego, w ramach niniejszej umowy Zamawiającemu, wyrobów medycznych zobowiązany jest niezwłocznie poinformować Zamawiającego o jakiejkolwiek zmianie w ww. zakresie, pod rygorem całkowitej i wyłącznej odpowiedzialności Wykonawcy za wszystkie mogące wystąpić dla Zamawiającego negatywne skutki powstałe w wyniku braku przekazania mu takich informacji.
10. Towar powinien być wydany w opakowaniu określonym Polskimi Normami lub normami branżowymi, a jeśli nie ma norm to w opakowaniu odpowiadającym właściwości towaru i środka transportu.
11. Wykonawca dostarczy Zamawiającemu wyroby medyczne z terminami ważności nie krótszymi niż 12 miesięcy licząc od dnia ich dostawy. Zamawiający zastrzega sobie prawo do odmowy przyjęcia dostawy zawierającej towar o krótszym niż wskazany w umowie terminie ważności.
12. **W przypadku stwierdzenia wad fizycznych lub braków ilościowych w dostarczonym towarze Zamawiający niezwłocznie w terminie nie dłuższym niż 7 dni roboczych od doręczenia dostawy zawiadomi o tym Wykonawcę oraz opisze wady lub braki w protokole dostawy. Wykonawca bezzwłocznie wymieni wadliwy towar na wolny od wad lub dostarczy brakujący towar zgodnie z zamówieniem (co do rodzaju, jakości i ilości)- w terminie nie dłuższym niż 7 dni roboczych od głoszenia danej reklamacji. W przypadku braku informacji o wadach lub brakach w wyżej wskazanym terminie, dostawę uznaję się jako wykonaną należycie, chyba że wada miała charakter ukryty i niemożliwą do sprawdzenia podczas przyjęcia dostawy**
13. Reklamacje Zamawiającego składane będą w formie faksu na nr:.....
14. Poza uprawnieniami wymienionymi w ust. 12 Zamawiający zastrzega sobie prawo, bez konieczności uprzedniego wzywania Wykonawcy do uzupełnienia braków ilościowych lub wymiany wadliwego towaru na wolny od wad, do nabycia zamawianych wyrobów medycznych u osoby trzeciej, jeżeli:

- Wykonawca nie dostarczył danego towaru w terminie, lub
- -Wykonawca dostarczył towar wadliwy lub niezgodny z opisem przedmiotu zamówienia zawartym w SIWZ.

Zamawiający w takim przypadku może zamówić u osoby trzeciej wyroby medyczne będące przedmiotem danego zamówienia w ramach niniejszej umowy, tożsame co do rodzaju i ilości, nawet bez konieczności zawiadamiania o tym Wykonawcy do wymiany wadliwych rzeczy, a Wykonawca zobowiązany będzie do zwrotu Zamawiającemu różnicy pomiędzy ceną z niniejszej umowy, a ceną zapłaconą na rzecz osoby trzeciej. Powyższe uprawnienia nie zamykają Zamawiającemu drogi do żądania kar umownych z tytułu zwłoki w dostawie towaru bądź z tytułu dostawy towaru wadliwego, przy czym za dzień zrealizowania dostawy przyjmuje się dzień jej zrealizowania przez osobę trzecią - wykonawcę zastępczego.

Zamawiający dokonuje zakupu u podmiotu trzeciego na własna odpowiedzialność i musi dopełnić wszelkiej staranności w celu potwierdzenia kompatybilności z urządzeniem w jakim będzie wykorzystywane

15. Postępowanie reklamacyjne określone w ust. 12-14 niniejszego paragrafu nie wyklucza uprawnień Zamawiającego z tytułu rękojmi przy sprzedaży określonych w kodeksie cywilnym. Zamawiający ma prawo wyboru reżimu reklamacji.

§2

1. Zamawiający zastrzega sobie możliwość wykonania auditu u Wykonawcy zgodnie z punktem 7.4.1 normy EN ISO 9001:2008 oraz normą ISO 27001:2007.
2. Wszelkie informacje, uzyskane przez Wykonawcę w związku z realizacją niniejszej umowy, Wykonawca powinien traktować jako poufne. Wykonawca zobowiązany

jest do zachowania poufności informacji w trakcie obowiązywania umowy oraz po jej zakończeniu.

3. Wykonawca zobowiązuje się do przestrzegania, w zakresie adekwatnym do przedmiotu niniejszej Umowy, Polityki Bezpieczeństwa Informacji obowiązującej u Zamawiającego.
4. W sytuacji, w której naruszenie poufności informacji lub Polityki Bezpieczeństwa Informacji spowoduje szkodę po stronie Zamawiającego, Wykonawca zobowiązany jest do jej naprawienia na zasadach ogólnych.

§3

1. Zamawiający zapłaci za zamówiony i dostarczony towar cenę brutto określoną w załączniku nr 1 do niniejszej umowy.
2. Wykonawca oświadcza, że jest podatnikiem podatku od towarów i usług VAT zobowiązanym do zapłaty i odprowadzenia tego podatku.
3. Zapłata za dostarczony na podstawie zamówienia towar nastąpi przelewem na konto bankowe Wykonawcy podane w doręczonej przez niego Zamawiającemu, prawidłowo wystawionej fakturze VAT, potwierdzającej dostawę towaru, w ciągu 60 dni od dnia jej otrzymania przez Zamawiającego.
4. Za dzień zapłaty uważa się dzień obciążenia rachunku Zamawiającego.
5. Termin płatności faktur dotyczących dostawy, w której został stwierdzony wadliwy towar, rozpoczyna swój bieg od dnia wymiany wadliwego towaru na wolny od wad. Dostawa faktur korygujących nastąpi razem z dostawą towaru wolnego od wad.
6. Faktura oraz inny dokument potwierdzający dostawę winny bezwzględnie obejmować sprzęt medyczny tylko z niniejszej umowy i zawierać wskazanie numeru niniejszej umowy oraz numeru zamówienia (zamówień), ~~daty ważności oraz numeru serii dostarczonego produktu~~ w związku z którymi nastąpiła dostawa.
7. Zamawiający oświadcza, że oszacował ilość zamawianego towaru z należytą starannością, w oparciu o dane z lat ubiegłych, jednakże ze względu na losowy charakter zapotrzebowania na wyroby medyczne, będące przedmiotem zamówienia (uzależnione od czynników niezależnych – tj. rodzaju schorzeń u pacjentów Zamawiającego) zastrzega sobie prawo zakupu mniejszej ilości towaru od ilości określonej w załączniku nr 1 do niniejszej umowy, a Wykonawca oświadcza, że wyraża na to zgodę i nie obciąży Zamawiającego jakimikolwiek negatywnymi konsekwencjami z tego tytułu.

§4

Zamawiający na podstawie art. 144 ust. 1 ustawy z dnia 29 stycznia 2004. prawo zamówień publicznych przewiduje możliwość dokonania zmiany w zawartej umowie w następujących sytuacjach:

1) wprowadzenia wyrobu medycznego nowego lub udoskonalonego, spełniającego parametry wymagane w SIWZ, pod warunkiem zachowania ceny jednostkowej netto na poziomie nie wyższym, niż wyrób objęty zamówieniem początkowym. Ewentualna zmiana wyrobu może być dokonana na pisemny wniosek każdej ze stron, poprzez zawarcie aneksu, w którym dotychczasowy wyrób zostanie wykreślony i zastąpiony wyrobem zmodyfikowanym lub udoskonalonym,
2) wycofania wyrobu medycznego z produkcji – Wykonawca ma obowiązek zapewnić dostarczenie wyrobu zamiennego o parametrach nie gorszych od produktu objętego umową pod warunkiem zachowania ceny jednostkowej netto na poziomie nie wyższym, niż wyrób objęty zamówieniem początkowym. Ewentualna zmiana wyrobu może być dokonana na pisemny wniosek Wykonawcy, poprzez zawarcie aneksu, mocą którego nastąpi wykreślenie z umowy wyrobu wycofanego z produkcji i zastąpienie go wyrobem zamiennym,
3) podwyższenia stawki podatku VAT przy czym zmianie ulega jedynie cena netto, cena brutto pozostaje bez zmian. Nowe stawki będą obowiązywać strony wraz z wejściem w życie przepisów je regulujących. Każdorazowa zmiana nie wymaga aneksu w formie pisemnej, ewentualnie strony mogą zawrzeć aneks porządkujący na wniosek Zamawiającego. W uzasadnionych wypadkach, na pisemny umotywowany wniosek

Wykonawcy strony mogą zawrzeć aneks, mocą którego zdecydują o podwyższeniu ceny brutto przy pozostawieniu ceny netto bez zmian; w takiej sytuacji strony mogą zdecydować również o odpowiednim do wzrostu stawki podatku VAT podwyższeniu wartości brutto całej umowy ze skutkiem od dnia określonego w treści aneksu.

4) obniżenia stawki podatku VAT przy czym zmianie ulega jedynie cena brutto, cena netto pozostaje bez zmian. Nowe stawki będą obowiązywać strony wraz z wejściem w życie przepisów je regulujących. Każdorazowa zmiana nie wymaga sporządzenia aneksu w formie pisemnej, ewentualnie strony mogą zawrzeć aneks porządkujący na wniosek Zamawiającego,
5) zmiany polegającej na zamianie jeszcze niewykorzystanego asortymentu, przewidzianego niniejszą umową, na inny asortyment z tej umowy, który został już wykorzystany, z zastrzeżeniem, iż całkowita wartość brutto umowy nie może ulec zmianie; zmiana nastąpi w formie aneksu do umowy w formie pisemnej pod rygorem nieważności,
~~6) zmiany przedmiotowej /wyrób medyczny zamienny/, dokonanej na czas określony, jeśli wystąpi przejściowy brak wyrobu z przyczyn leżących po stronie producenta, przy jednoczesnym dostarczeniu wyrobu zamiennego o parametrach nie gorszych od wyrobu objętego umową oraz przy zachowaniu ceny jednostkowej dotychczasowego wyrobu lub ceny niższej; zmiana nastąpi w formie aneksu do umowy w formie pisemnej pod rygorem nieważności, a za pisemną zgodą Kierownika Apteki Szpitalnej – bez konieczności zawarcia aneksu, jednakże z dokładnym określeniem czasu trwania zmiany, charakterystyki wyrobu zamiennego oraz jego ceny jednostkowej.~~
7) W przypadku niewyczerpania całości asortymentu określonego w Załączniku nr 1 w okresie, na jaki umowa została zawarta, okres ten może ulec przedłużeniu o czas określony, nie dłuższy niż 6 miesięcy. Zmiana istotnych postanowień umowy, wymaga zgody obu stron umowy wyrażonej w formie pisemnej pod rygorem nieważności (aneks do umowy).

§5

1. Wykonawca zobowiązany jest do informowania Zamawiającego o dotyczących go zmianach, w szczególności o zmianie organizacyjnej Wykonawcy, przekształceniu, zmianie formy prawnej prowadzonej przez Wykonawcę działalności gospodarczej, zmianie adresu siedziby firmy lub zmianie adresu zamieszkania właściciela lub współwłaściciela firmy. Niepowiadomienie przez Wykonawcę o zmianach nie będzie skutkować jakimikolwiek negatywnymi konsekwencjami dla Zamawiającego.
2. Osobą odpowiedzialną merytorycznie za realizację umowy ze strony Zamawiającego jest Kierownik Apteki Szpitalnej mgr Anna Wieczorek lub osoba przez nią upoważniona.

§6

Dla dokonania czynności skutkującej zmianą wierzyciela Zamawiającego wymagana jest uprzednia zgoda podmiotu tworzącego zgodnie z art. 54 ust. 5 ustawy o działalności leczniczej z dnia 15 kwietnia 2011 r. Dodatkowo, cesja wierzytelności z niniejszej umowy, jak również oddanie wierzytelności w zarząd osobie trzeciej, wymaga uprzedniej pisemnej zgody Zamawiającego pod rygorem nieważności.

§7

1. Wykonawca zobowiązuje się do zapłaty Zamawiającemu kar umownych z następujących tytułów i w wysokościach:

a) w razie wystąpienia zwłoki w dostawie towaru § 1 pkt. 5 – w wysokości **0,2%** wartości brutto niedostarczonego towaru za każdy dzień zwłoki;
b) za dostarczenie towaru z wadami – **0,2%** wartości brutto towaru dostarczonego z wadami za każdy dzień zwłoki, licząc od dnia dostawy, aż do dnia wymiany wadliwego towaru na zgodny z zamówieniem co do jakości i ilości;
c) za odstąpienie od umowy z przyczyn, za które ponosi odpowiedzialność Wykonawca – w wysokości 10% wartości brutto całej umowy (według stanu na dzień odstąpienia);

d) za niedostarczenie dokumentów w terminie 30 dni o których mowa w § 1 ust. 8 – w wysokości 20% wartości brutto całej umowy (według stanu na dzień naruszenia);.

2. Jeżeli szkoda Zamawiającego, spowodowana okolicznościami stanowiącymi podstawę naliczenia kar umownych, przewyższa wysokość naliczonych kar, Zamawiający może dochodzić na zasadach ogólnych odszkodowania uzupełniającego.

§8

1. Zamawiającemu przysługuje prawo do rozwiązania umowy za 7 dniowym wypowiedzeniem w następujących sytuacjach:
   a) w razie niewykonania lub powtarzającego się nienależytego wykonania umowy przez Wykonawcę, w szczególności w powtarzających się opóźnień w dostawie towaru (co najmniej 4 razy) lub powtarzających się dostaw towaru wadliwego (co najmniej 4 razy).
   b) w razie pogorszenia sytuacji finansowej Zamawiającego w trakcie trwania umowy skutkującej niemożnością dalszej jej realizacji.
2. Zgodnie z art. 145 ust. 1 ustawy Prawo zamówień Publicznych, Zamawiający ma prawo do odstąpienia od umowy w terminie 30 dni od powzięcia wiadomości o istotnej zmianie okoliczności powodującej, iż wykonanie umowy nie leży w interesie publicznym, czego nie można było przewidzieć w chwili zwarcia umowy.

§9

1. W kwestiach spornych wynikłych w związku z treścią lub realizacją niniejszej umowy strony będą dążyły do polubownego załatwienia sprawy, a gdy okaże się to niemożliwe, miejscowo właściwym będzie sąd powszechny właściwy dla Zamawiającego.
2. W sprawach nieuregulowanych niniejszą umową, zastosowanie mają przepisy Kodeksu Cywilnego i Ustawy Prawo Zamówień Publicznych. Strony wyłączają jednak między sobą obowiązywanie art. 552 k.c.
3. Wykonawca oświadcza, że jest mu znany stan majątkowy Zamawiającego w rozumieniu dyspozycji z art. 490 ust. 2 ustawy k.c.
4. Umowę sporządzono w czterech jednobrzmiących egzemplarzach, po dwa egzemplarze dla każdej ze stron.
5. Załączniki do umowy stanowią jej integralną część:

Załączniki:

Załącznik nr 1 – formularz asortymentowo – cenowy;
Załącznik nr 2 – wpis do Krajowego Rejestru Sądowego lub innego rejestru;
Załącznik nr 3 – dokument dotyczący nadanie Wykonawcy numeru NIP;
Załącznik nr 4 – dokument dotyczący nadanie Wykonawcy numeru REGON.

Wykonawca **Zamawiający**

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.

2. Deklaracja Polityki Bezpieczeństwa Informacji

Dyrektor Szpitala rozumiejąc, że informacja jest jednym z najważniejszych aktywów każdej organizacji, wdrożył system zarządzania bezpieczeństwem informacji, którego głównym celem jest zapewnienie poufności, integralności, dostępności informacji oraz zabezpieczenie przed nieautoryzowanym dostępem lub zniszczeniem zasobów, które biorą udział w przechowywaniu, przesyłaniu oraz przetwarzaniu informacji. Środki podjęte do ochrony zasobów oraz zakres ochrony są odpowiednie do zakresu przetwarzanych informacji oraz uwzględniają cele biznesowe Szpitala.

Szpital zapewnia bezpieczeństwo informacji poprzez:

- ✓ zarządzanie ryzykiem, w ramach którego przeprowadza się ocenę wartości zasobów i klasyfikację informacji, identyfikację poziomów zagrożeń i ich konsekwencji; pod uwagę bierze się takie kryteria jak ryzyko, skutki oraz miejsce utraty informacji; podejmuje się również działania mające na celu zdefiniowanie sposobów zarządzania zabezpieczeniami zasobów,
- ✓ zarządzanie zmianami, w ramach którego prowadzi się analizę zmian pod względem ich wpływu na poziom bezpieczeństwa oraz zapewnienie pełnej koordynacji podczas wprowadzania zmian,
- ✓ zarządzanie ciągłością działania Szpitala przez określenie, wdrożenie i utrzymanie Planu postępowania na wypadek sytuacji nadzwyczajnej na terenie Szpitala.

Główne cele systemu zarządzania bezpieczeństwem informacji to:

- ✓ zapewnienie dostępności do informacji osobom upoważnionym,
- ✓ zabezpieczenie informacji, dokumentów, systemów przetwarzających informacje przed nieautoryzowanym dostępem, modyfikacją lub zniszczeniem,
- ✓ minimalizowanie ryzyka utraty informacji,
- ✓ zaangażowanie wszystkich pracowników w ochronę informacji,
- ✓ zwiększanie świadomości pracowników,
- ✓ monitorowanie korzystania z danych osobowych oraz medycznych na wszystkich etapach ich przetwarzania przed nieautoryzowanym dostępem, zmianą, kopiowaniem, zniszczeniem,
- ✓ zapewnienie zgodności z prawem obowiązującym na terytorium RP w zakresie ochrony danych osobowych oraz zgodności z umowami.

Dyrekcja Szpitala podejmuje działania związane z zapewnieniem środków niezbędnych do realizacji Polityki Bezpieczeństwa Informacji (ogólnej i szczegółowej). W Szpitalu został powołany Komitet ds. Bezpieczeństwa, którego głównymi zadaniami są: wyznaczanie i aktualizacja celów stosowania zabezpieczeń, technik zabezpieczeń oraz zarządzanie klasyfikacją informacji i szacowaniem ryzyka. W skład Komitetu wchodzą pracownicy z komórek organizacyjnych Szpitala mające istotny wpływ na poziom bezpieczeństwa informacji w Szpitalu.

Role, uprawnienia i odpowiedzialności osób odpowiedzialnych za zarządzaniem bezpieczeństwem informacji zostały określone w Załączniku nr 5 do niniejszego dokumentu oraz pozostałej dokumentacji bezpieczeństwa informacji. Pracownicy Szpitala oraz podmioty zewnętrzne są zobowiązani do zapoznania się i respektowania postanowień dokumentacji bezpieczeństwa informacji.

Dla realizacji celów opisanych w deklaracji stosowania mających za zadanie zapewnienie skutecznego funkcjonowania systemu zarządzania bezpieczeństwem informacji zgodnego z wymaganiami normy PN-ISO/IEC 27001:2007 ustanowione zostały zabezpieczenia. Zbiór zabezpieczeń, powodów stosowania tych zabezpieczeń jak i cele wybranych do stosowania w Szpitalu zabezpieczeń zostały zebrane oraz wymienione w „Deklaracji stosowania" stanowiącej Załącznik nr 6 do niniejszego dokumentu. Za nadzorowanie jej zmian, aktualizację oraz nadzór nad realizacją wymogów okresowego monitorowania odpowiedzialny jest Pełnomocnik ds. Bezpieczeństwa.

2.1 System zabezpieczeń danych osobowych (środki techniczne i organizacyjne)

Każdy ma prawo do ochrony dotyczących go danych osobowych. Prawo to reguluje ustawa o ochronie danych osobowych oraz rozporządzenie MSWiA w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

Instrukcja zarządzania systemem informatycznym przetwarzającym dane osobowe zawiera:

- ✓ wykaz budynków tworzących obszar, w którym przetwarzane są dane osobowe,
- ✓ wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych,
- ✓ opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi określenie sposobu przepływu danych pomiędzy poszczególnymi systemami.

Dostęp do danych osobowych mogą mieć tylko osoby posiadające pisemne, imienne upoważnienia. Osoby upoważnione mają dostęp do danych osobowych zgodnie z zasadą przywilejów koniecznych, tylko w takim zakresie w jakim jest im to niezbędne do wykonywania obowiązków służbowych.

Dane osobowe, powinny być zabezpieczone zgodnie z ustanowionymi zasadami bezpieczeństwa, a każdy z użytkowników powinien zachować szczególną ostrożność przy przetwarzaniu wszelkich danych osobowych

stosując się do zasad określonych w Regulaminie użytkownika systemu informatycznego - Załącznik nr 7 do niniejszego dokumentu.

Zbiór zasad ustalonych w dokumentacji SZBI ma zastosowanie do wszystkich zbiorów danych osobowych administrowanych przez Szpital w szczególności do:

- ✓ wszystkich istniejących, wdrażanych obecnie lub w przyszłości systemów informatycznych, w których przetwarzane są lub będą dane osobowe podlegające ochronie,
- ✓ danych osobowych (wrażliwych) przetwarzanych w dowolnej formie (np. elektronicznej, papierowej),
- ✓ danych osobowych zarówno w przypadku, gdy Szpital jest administratorem danych, jak i w sytuacji, gdy przetwarza dane powierzone mu na podstawie umów zawartych w trybie art. 31 ustawy o ochronie danych osobowych,
- ✓ wszystkich nośników informacji, np. papierowych, magnetycznych, optycznych itp., na których są lub będą znajdować się dane osobowe podlegające ochronie,
- ✓ wszystkich pomieszczeń, w których są lub będą przetwarzane dane osobowe podlegające ochronie,
- ✓ wszystkich pracowników w rozumieniu przepisów Kodeksu Pracy, stażystów, praktykantów i innych osób (strony trzecie) mających dostęp do danych osobowych podlegających ochronie.

Szczegółowe zasady wydawania upoważnień, nadawania, zmiany i cofania uprawnień określone są w Procedurze PR-04 QBP-02 System kontroli dostępu.

W przypadku naruszenia zasad dotyczących bezpieczeństwa przetwarzanych informacji zawierających dane osobowe należy postępować zgodnie z Instrukcją Postępowania w sytuacji naruszenia ochrony danych osobowych zawartą w Rozdziale 8 niniejszego dokumentu.

3. Organizacja bezpieczeństwa informacji

Kluczowe z punktu widzenia funkcjonowania systemu zarządzania bezpieczeństwem informacji jest odpowiednie ustalenie odpowiedzialności i obowiązków stron odpowiedzialnych za funkcjonowanie systemu. Niniejsza Polityka określa podstawowe obowiązki pracowników odpowiedzialnych za bezpieczeństwo informacji i zasobów.

3.1 Role w ramach struktury organizacyjnej

Zarządzanie bezpieczeństwem informacji w Szpitalu odbywa się w oparciu o ustanowione poniżej role (funkcje). Obowiązkiem Szpitala jest wskazanie konkretnego pracownika (stanowisko), odpowiedzialnego ze realizację działań dla ustanowionych ról. Dla każdej ustanowionej roli przypisano obszar działań dotyczących bezpieczeństwa informacji. Wykaz osób pełniących kluczową rolę w ramach SZJiZBI zamieszczono w Załączniku nr 3 do niniejszego dokumentu.

3.1.1 Dyrektor Szpitala

Dyrektor Szpitala odpowiedzialny jest za zaangażowanie w proces utrzymania systemu zarządzania bezpieczeństwem informacji oraz podejmowanie działań w celu zapewnienia zasobów niezbędnych do funkcjonowania tego systemu. W szczególności do obowiązków Dyrektora należy:

- ✓ zatwierdzenie Polityki Bezpieczeństwa Informacji wraz z dokumentami towarzyszącymi (regulaminy, procedury, instrukcje, plany, deklaracja stosowania),
- ✓ zatwierdzenie zmian Polityki Bezpieczeństwa Informacji wraz z dokumentami towarzyszącymi,
- ✓ ustanowienie struktury zarządzania bezpieczeństwem informacji – powołanie Komitetu ds. Bezpieczeństwa,
- ✓ powołanie Pełnomocnika ds. Bezpieczeństwa oraz administratorów poszczególnych obszarów bezpieczeństwa,
- ✓ zatwierdzanie wyników analizy ryzyka i planów postępowania z ryzykiem,
- ✓ podejmowanie działań w celu zapewnienia dostępności zasobów niezbędnych do utrzymania funkcjonowania systemu zarządzania bezpieczeństwem informacji,
- ✓ zapewnienie finansowania przedsięwzięć z zakresu bezpieczeństwa informacji,
- ✓ podejmowanie strategicznych decyzji w zakresie bezpieczeństwa informacji.

3.1.2 Komitet ds. Bezpieczeństwa

Komitet ds. Bezpieczeństwa odpowiedzialny jest za koordynowanie działań związanych z bezpieczeństwem informacji przez reprezentantów różnych obszarów Szpitala pełniących odpowiednie role. Obowiązki oraz uprawnienia członków Komitetu ds. Bezpieczeństwa zostały określone w Załączniku nr 5 do niniejszego dokumentu.

3.1.3 Autor publikacji

Autorem publikacji jest każda osoba, która powoduje utrwalenie informacji w formie papierowej, elektronicznej lub innej. Autor każdej publikacji odpowiedzialny jest za:

- ✓ określenie klasy dokumentu zgodnie z przyjętą klasyfikacją informacji,
- ✓ oznaczenie dokumentu zgodnie z wymaganiami Polityki Bezpieczeństwa Informacji i wymaganiami klasyfikacji informacji.

Minimalne wymagania dotyczące kompetencji: szkolenie w zakresie systemu zarządzania bezpieczeństwem informacji.

3.1.4 Redaktor publikacji

Redaktorem publikacji jest każdy pracownik Szpitala, który zleca lub nadzoruje utrwalenie informacji. Redaktor każdej publikacji odpowiedzialny jest za:

- ✓ weryfikację informacji przeznaczonych do publikacji pod kątem zgodności z przyjętą klasyfikacją informacji,
- ✓ zatwierdzanie informacji do publikacji w środkach publicznie dostępnych,
- ✓ okresową weryfikację publikacji i jej aktualności w środkach publicznie dostępnych (w celu ograniczenia nieautoryzowanej treści publikacji).

Minimalne wymagania dotyczące kompetencji: szkolenie w zakresie systemu zarządzania bezpieczeństwem informacji.

3.1.5 Kierownicy komórek organizacyjnych w Szpitalu

Kierownicy poszczególnych komórek organizacyjnych w Szpitalu w ramach udziału w procesie zarządzania bezpieczeństwem informacji odpowiedzialni są za:

- ✓ wdrażanie Polityki Bezpieczeństwa Informacji i planów postępowania z ryzykiem w ramach kompetencji w podległych im komórkach organizacyjnych,
- ✓ podejmowanie działań w celu zapewnienia zasobów niezbędnych do utrzymania funkcjonowania systemu zarządzania bezpieczeństwem informacji,
- ✓ podejmowania działań w celu określenia zasad właściwego korzystania z zasobów i informacji w ramach podległej komórki organizacyjnej,
- ✓ nadzór nad bezpieczeństwem informacji w ramach kompetencji w podległych im komórkach organizacyjnych,
- ✓ uczestnictwo w analizie ryzyka bezpieczeństwa informacji w zakresie podległych im komórek i wdrażanie działań wynikających z przeprowadzonej analizy.

3.1.6 Pracownik (użytkownik)

Każdy pracownik odpowiedzialny jest za:

- ✓ stosowanie procedur wynikających z dokumentacji SZBI,
- ✓ jakość świadczonych usług dla klientów oraz tworzenie bezpiecznego środowiska pracy,
- ✓ wypełnianie swoich obowiązków określonych w dokumentacji przechowywanej w aktach osobowych,
- ✓ stosowanie i przestrzeganie przyjętych zasad i postanowień określonych w dokumentacji SZBI,
- ✓ przestrzeganie zasad ochrony danych osobowych określonych w Polityce Bezpieczeństwa Informacji i dokumentach z nią związanych,
- ✓ przetwarzanie danych osobowych zgodnie z celami ich przetwarzania,
- ✓ zapewnienie bezpieczeństwa danych osobowych, do których uzyskują dostęp w ramach pełnienia obowiązków służbowych,
- ✓ zachowanie szczególnej staranności w trakcie wykonywania operacji przetwarzania danych osobowych w celu ochrony interesów osób, których te dane dotyczą,
- ✓ informowanie Administratora Bezpieczeństwa lub Pełnomocnika ds. Bezpieczeństwa o wszelkich zauważonych nieprawidłowościach skutkujących obniżeniem poziomu bezpieczeństwa (poufność, integralność, dostępność) danych osobowych,
- ✓ współpracę z Komitetem Bezpieczeństwa w zakresie bezpieczeństwa informacji.

3.2 Upoważnienia i zgody

Przez zgodę rozumiane jest wyrażenie aprobaty przełożonego lub wskazanej w dokumentacji bezpieczeństwa informacji osoby na wykonanie konkretnej czynności przez określoną osobę.

Przez czasowe upoważnienie rozumiane jest wyrażenie aprobaty przełożonego lub wskazanej w dokumentacji bezpieczeństwa informacji osoby na wykonywanie określonego rodzaju czynności przez określoną osobę w oznaczonym okresie czasu.

Przez stałe upoważnienie rozumiane jest wyrażenie aprobaty przełożonego lub wskazanej w dokumentacji bezpieczeństwa informacji osoby na wykonywanie określonego rodzaju czynności przez określoną osobę aż do odwołania upoważnienia.

Pod nieobecność przełożonego lub wskazanej w dokumentacji bezpieczeństwa informacji osoby upoważnienie lub zgodę może wydać osoba upoważniona do zastępstwa.

Wszędzie tam, gdzie w niniejszej Polityce mowa jest o udzielaniu zgody (upoważnienia) w formie pisemnej należy przez to rozumieć pismo podpisane odręcznie, wiadomość poczty elektronicznej lub wpis do systemu informatycznego mającego funkcjonalność zapisywania i prezentowania osoby (lub konta informatycznego o uwierzytelnionym dostępie), która dokonała wpisu.

3.3 Porozumienia i kontakty ze stronami zewnętrznymi

Współpraca Szpitala z podmiotem zewnętrznym może mieć wpływ na funkcjonowanie kluczowych elementów systemu zarządzania bezpieczeństwem informacji. Współpraca ta realizowana jest w oparciu o zawartą z tym podmiotem umowę. Szczegółowe zasady dotyczące tworzenia umów reguluje Zarządzenie Dyrektora Nr 39/2010 w sprawie wprowadzenia Instrukcji dotyczącej "Zasad tworzenia, obiegu i rejestracji umów zawieranych przez Wojewódzki Szpital Specjalistyczny im. M. Kopernika w Łodzi. Do zawierania umów z podmiotami zewnętrznymi upoważniony jest jedynie Dyrektor Szpitala a pod jego nieobecność upoważniony Zastępca.

Ogólne zasady dotyczące współpracy z dostawcami zostały określone w procedurze systemowej PR-07 QBP-01 Realizacja dostaw.

W kontaktach z podmiotami zewnętrznymi Szpital reprezentowany jest przez Dyrektora lub osobę upoważnioną do realizacji określonego zadania.

3.4 Procedury systemu zarządzania bezpieczeństwem informacji

Dokumentacja bezpieczeństwa informacji jest nadzorowana przez Pełnomocnika ds. Bezpieczeństwa i jest dostępna dla wszystkich zainteresowanych osób (pracowników Szpitala) z wyjątkiem dokumentów o charakterze poufnym. Aktualne dokumenty są umieszczone w intranecie Szpitala.

Zasady określone w Polityce Bezpieczeństwa Informacji są realizowane są w Szpitalu zgodnie z procedurami systemowymi określonymi w Księdze Jakości Zintegrowanego Systemu Zarządzania Jakością i Zarządzania Bezpieczeństwem Informacji.

3.4.1 Nadzór nad dokumentami i zapisami

Wszystkie dokumenty systemu zarządzania bezpieczeństwem informacji powinny być aktualne, zatwierdzone i dostępne dla uprawnionych pracowników. Wszystkie egzemplarze dokumentacji w postaci papierowej należy traktować jako nadzorowane. Egzemplarze w postaci elektronicznej należy traktować jako nienadzorowane, chyba, że w jawny sposób są oznaczone jako nadzorowane.

W każdym obszarze działalności wyszczególnione zostały zapisy (dowody wykonania określonych działań), wskazane zostały osoby odpowiedzialne za nadzór nad zapisami. Kierownicy poszczególnych komórek organizacyjnych w Szpitalu pełnią nadzór kierowniczy nad zapisami – kontrolują, by zapisy wykonywano w sposób właściwy.

Dokumentacja bezpieczeństwa informacji jest opracowana zgodnie wymogami szczegółowej procedury nadzoru nad dokumentami i zapisami. Dla zapewnienia jednolitego sposobu tworzenia, ewidencjonowania i przechowywania dokumentów należy zapewnić zgodność Instrukcji Kancelaryjnej z wymaganiami szczegółowymi procedur.

Wszystkie dokumenty zawierające dane osobowe (w tym dane medyczne) podlegają ochronie zgodnie z zasadami określonymi w Załączniku nr 4 – Klasyfikacja informacji. Zasady te dotyczą zarówno oryginałów jak również każdej kopii, niezależnie od rodzaju nośnika na jakim zostały utrwalone.

3.4.2 Działania zapobiegawcze, korekcyjne oraz korygujące, postępowanie z incydentem

Skuteczne funkcjonowanie systemu zarządzania bezpieczeństwem informacji powinno opierać się na wiedzy odnośnie występowania podatności, zagrożeń, zdarzeń oraz incydentów bezpieczeństwa. Dlatego też niezbędne jest zgłaszanie informacji o zagrożeniach, zdarzeniach oraz incydentach. Uzyskiwane informacje służą do podejmowania działań naprawczych i doskonalących (korygujących lub zapobiegawczych). Ich celem jest zapewnienie szybkiej, efektywnej i uporządkowanej reakcji na zdarzenia związane z bezpieczeństwem informacji, w tym wyjaśnienie przyczyn, przypisania odpowiedzialności i określenia wniosków co do zakresu działań zapobiegawczych w przyszłości. Obowiązujące w tym zakresie zasady zostały spisane w Procedurze PR-03 QBP-002/S Nadzór nad niezgodnościami. Działania zapobiegawcze, korekcyjne oraz korygujące.

3.4.3 Audity wewnętrzne

Audity wewnętrzne służą weryfikacji czy ustanowiony Zintegrowany System Zarządzania jest zgodny z wymaganiami określonych norm i standardów, czy działania przebiegają zgodnie z opracowaną dokumentacją systemu zarządzania oraz czy system ten jest skutecznie wdrożony i utrzymywany. Audyty wewnętrzne są planowane i przeprowadzane zgodnie z Procedurą systemową PR-03 QBP-003/S Audit wewnętrzny.

3.4.4 Kompetencje, podnoszenie świadomości oraz szkolenia

Wszyscy pracownicy Szpitala wykonujący swoje zadania mają wpływ na jakość świadczonych usług oraz bezpieczeństwo przetwarzanych informacji. Dlatego wszyscy pracownicy powinni posiadać odpowiednie kompetencje do wykonywania zadań oparte na odpowiednim wykształceniu, szkoleniach, umiejętnościach i doświadczeniu. Wymagania te zostały określone w Procedurze PR-04 QBP-01. Dla zapewnienia ciągłego doskonalenia i osiągania optymalnych efektów w działalności Szpitala, prowadzone są okresowe szkolenia zgodnie z w/w procedurą.

3.4.5 Nadzorowanie zakupów

Proces zakupów powinien być zgodny z przepisami prawnymi regulowanymi przez prawo zamówień publicznych. Procedura dokonywania zakupów w Szpitalu odbywa się na podstawie opracowanego Regulaminu Zamówień Publicznych.

Podczas realizacji umów zakupionych towarów i usług odbywa się weryfikacja dostarczonego wyrobu lub usługi pod kątem jej zgodności z wymaganiami specyfikacji istotnych warunków zamówienia (SIWZ) oraz zgodności z warunkami umowy. Proces ten odbywa się zgodnie z Procedurą systemową PR-07 QBP-01 Realizacja dostaw.

3.4.6 Przeglądy kierownictwa

Ustanowiony Zintegrowany System Zarządzania wymaga, aby kierownictwo Szpitala dokonywało regularnych przeglądów systemu. Głównym celem realizacji przeglądu jest zapoznanie kierownictwa z aktualnym stanem systemu zarządzania oraz podjęcie decyzji związanych z jego dalszym funkcjonowaniem. Tematyka ta została szczegółowo opisana w Księdze ZSZJiBI.

3.4.7 Aktywa

Pracownikom powierza się aktywa Szpitala w celu realizacji zleconych im zadań. Aktywa są tym wszystkim, co stanowi wartość dla Szpitala np. narzędzia, urządzenia, materiały, wyposażenie itp. Za znajdujące się w komórce organizacyjnej aktywa odpowiada gestor. Gestor to kierownik komórki organizacyjnej Szpitala odpowiedzialny za funkcjonowanie aktywów znajdujących się na wyposażeniu komórki organizacyjnej oraz za określenie zasad dostępu i zasad akceptowalnego użycia przez pracowników. Dopuszczenie do użytkowania aktywów następuje według zasad określonych w Procedurach PR-06 QBP-01 Nadzór nad aparaturą medyczną oraz PR-05 QBP-02/E Nadzór nad sprzętem komputerowym i oprogramowaniem. Pracownicy mogą wykorzystywać aktywa Szpitala zgodnie z nich przeznaczeniem i za zgodą gestora. Pracownicy zobowiązani są do poszanowania powierzonych im aktywów oraz korzystania z nich w należyty sposób. Z chwilą rozwiązania umowy z pracownikiem gestor zobowiązany jest do rozliczenia pracownika z powierzonych mu aktywów.

Sposób wykorzystania zasobów przydzielonych do użytku prywatnego może podlegać monitorowaniu polegającego m.in. na monitorowaniu użycia komputera oraz aplikacji, śledzeniu aktywności sieciowej pracownika. Upoważnieni pracownicy Działu Informatyki mogą weryfikować wykorzystanie komputerów służbowych do realizacji zadań nie związanych bezpośrednio z pracą np. przeglądanie poczty prywatnej, korzystanie z portali społecznościowych, pobieranie nielegalnych plików. Wszystkie zasoby powierzone pracownikom nie mogą być traktowane jako zasoby prywatne.

Ze względów bezpieczeństwa teren Szpitala (wewnątrz i na zewnątrz) jest monitorowany przy użyciu kamer przez służby odpowiedzialne za ochronę obiektu. Nagrania z monitoringu mogą być użyte jako materiał dowodowy w postępowaniu wyjaśniającym. Archiwizację nagrań i nadzór nad nimi zgodnie z zawartą umową sprawuje podmiot zewnętrzny świadczący usługi z zakresu ochrony Szpitala.

3.4.8 Inwentaryzacja aktywów

Okresowo nie rzadziej niż raz na dwa lata przeprowadzana jest inwentaryzacja aktywów. Inwentaryzację aktywów należy przeprowadzać poprzez identyfikację procesów biznesowych (głównych działań) oraz aktywów biorących udział w tych procesach. Aktywa mogą być podzielone na aktywa materialne (wyposażenie, zasoby) i aktywa niematerialne (informacje, dokumenty). Każda informacja i zasób powinny mieć przypisanego właściciela informacji lub właściciela zasobu odpowiedzialnego za określenie zasad postępowania z informacją lub zasobem. Wyniki inwentaryzacji aktywów są kluczowym elementem poprawnie przeprowadzonej analizy ryzyka. Za przeprowadzanie okresowych inwentaryzacji odpowiedzialni są wyznaczeni przez Dyrektora Szpitala pracownicy. Za nadzorowanie procesu inwentaryzacji istotnych z punktu widzenia bezpieczeństwa informacji odpowiedzialny jest Pełnomocnik ds. Bezpieczeństwa. Wykaz pogrupowanych aktywów wraz z przypisanym gestorem zawarty jest w analizie ryzyka.

3.4.9 Analiza ryzyka

Głównym celem analizy ryzyka bezpieczeństwa informacji jest wyznaczenie właściwych kierunków działania kierownictwa oraz określenia priorytetów dla zarządzania zabezpieczeniami. Wyniki analizy ryzyka prowadzą do opracowania planu postępowania z ryzykiem. Poszczególne etapy analizy oraz sposób przeprowadzania analizy reguluje stosowna procedura.

3.4.10 System Kontroli dostępu

Celem podstawowym systemu zarządzania bezpieczeństwem informacji jest zapewnienie, że dostęp do informacji (która nie jest publicznie dostępna) oraz poszczególnych stref bezpieczeństwa jest możliwy tylko dla osób upoważnionych. W tym celu utworzony został plan praw dostępu. Zasady dotyczące zarządzania uprawnieniami dostępu do pomieszczeń i systemu teleinformatycznego opisane zostały w Procedurze PR-04 QBP-02 System kontroli dostępu.

3.4.11 Monitorowanie zabezpieczeń systemu zarządzania bezpieczeństwem informacji

Jedną z metod zabezpieczania aktywów Szpitala jest stosowanie zabezpieczeń mających na celu zmniejszenie ryzyka związanego ze zidentyfikowanym zagrożeniem. Skuteczność funkcjonowania

zabezpieczeń determinuje stosowanie mechanizmów okresowej kontroli i monitorowania stanu zabezpieczeń. Pełnomocnik ds. Bezpieczeństwa w porozumieniu z administratorami poszczególnych obszarów bezpieczeństwa informacji odpowiedzialny jest za zdefiniowanie miar skuteczności wybranych zabezpieczeń oraz określenie sposobu oceny tych miar. Zabezpieczenia wraz z okresami monitorowania i wyborem osób odpowiedzialnych za monitorowanie zostały określone w kartach celów. Osoby odpowiedzialne odnotowują w karcie sposób i stopień realizacji celu. Karty podlegają okresowej weryfikacji wg określonych terminów realizacji.

Monitorowanie funkcjonowania bezpieczeństwa informacji w obszarach bezpieczeństwa teleinformatycznego, fizycznego i osobowego Szpitala realizowane przez poszczególnych administratorów bezpieczeństwa odbywa się zgodnie z zasadami określonymi w Załączniku nr 5 do niniejszego dokumentu.

4. Klasyfikacja, ochrona informacji i dokumentów

Klasyfikowanie informacji ma na celu zapewnienie właściwego poziomu jej ochrony w stosunku do znaczenia informacji dla Szpitala. Tym samym możliwa jest optymalizacja nakładów związanych ze zbyt kosztowną ochroną informacji.

Klasyfikacja informacji obejmuje wszystkie informacje, z jakimi mają do czynienia pracownicy Szpitala. Dzięki poprawnie przeprowadzonej identyfikacji informacji możliwe jest zidentyfikowanie właścicieli informacji, autorów, redaktorów informacji oraz innych podmiotów współuczestniczących w przetwarzaniu informacji. Określenie grona pracowników mających dostęp do informacji, jak i określenie wagi informacji pod kątem wymagań dla integralności, dostępności i poufności pozwala na przyjęcie uzasadnionej biznesowo klasyfikacji informacji.

Klasyfikacja informacji jest jedną z form określenia sposobu postępowania z informacją i jej ochroną. Przestrzeganie klasyfikacji informacji oraz postępowanie zgodne z wytycznymi dotyczącymi klasyfikacji informacji jest kluczowe z punktu widzenia bezpieczeństwa informacji.

4.1 Ogólne zasady postępowania z informacjami i dokumentami.

Określenie klasy dokumentu powinno być dokonane na podstawie zasad klasyfikowania informacji opisanych w Załącznika nr 4 do niniejszego dokumentu. Za zarządzanie klasyfikacją informacji odpowiedzialny jest Pełnomocnik ds. Bezpieczeństwa.

Określenie klasy i jej oznaczenie musi być dokonane na jak najwcześniejszym etapie prac nad dokumentem, nie później jednak niż w chwili udostępnienia lub przekazania dokumentu innym osobom.

Autor dokumentu jest zobowiązany do określenia klasy dokumentu oraz odpowiedniego oznaczenia dokumentu lub umieszczenia go w miejscu właściwym dla klasy dokumentu w momencie tworzenia dokumentu.

Adresat dokumentu, jeśli dokument nie został dotychczas oznaczony, jest zobowiązany do określenia klasy dokumentu i odpowiedniego oznaczenia lub umiejscowienia dokumentu, właściwego dla klasy dokumentu.

Zakazana jest zmiana klasy informacji lub dokumentu bez zgody autora dokumentu. W przypadku informacji lub dokumentów „poufnych" zakazana jest również zmiana listy dostępu bez zgody autora dokumentu.

Domyślną klasą dokumentu niesklasyfikowanego (który nie jest oznaczony etykietą, nie jest umieszczony w miejscu oznaczonym etykietą) lub dokumentu, który nie jest w oczywisty sposób dokumentem poufnym (np. dokumentacja medyczna lub inna zawierająca dane osobowe), jest klasa „publicznie dostępny". Dokumenty zewnętrzne, wpływające do Szpitala nie są sklasyfikowane, dlatego adresat dokumentu po zapoznaniu się z treścią określa jego klasę.

Pracownik przekazujący lub udostępniający dokument podmiotom zewnętrznym zobowiązany jest do wyraźnego oznaczenia dokumentu adnotacją, iż jest to dokument chroniony chyba, że udostępnianie lub przekazywanie odbywa się na podstawie umowy, która stanowi inaczej lub gdy właściciel dokumentu wyrazi zgodę na udostępnienie lub przekazanie bez takiej adnotacji. Zakazane jest przekazanie dokumentu (lub informacji) innego niż dokument jawny w rozumieniu wewnętrznego regulaminu mediom bez zgody osób odpowiedzialnych za kontakty z mediami. Zgoda taka powinna mieć formę pisemną.

Informacje niebędące dokumentami (a więc nieutrwalone – np. informacje przekazywane ustnie) podlegają takiej samej ochronie jakiej podlegałyby, gdyby zostały utrwalone w formie dokumentów. W szczególności informacje sklasyfikowane jako „do użytku wewnętrznego" lub „poufne" podlegają takiej samej ochronie jak dokumenty z daną klasą informacji, zarówno przy kontaktach wewnątrz Szpitala, jak i w kontaktach z osobami spoza niego.

Każdy pracownik jest zobowiązany do niezwłocznego zgłaszania osobie upoważnionej do reagowania na incydenty, wszelkie wykryte lub podejrzewane przypadki naruszenia zasad postępowania z dokumentami. W szczególności każdy pracownik jest zobowiązany do niezwłocznego zgłaszania znalezienia dokumentu niejawnego, pozostającego bez nadzoru w miejscu nieprzeznaczonym na przechowywanie takich dokumentów.

Zasady dotyczące okresu przechowywania dokumentów oraz nadzoru nad nimi zostały określone w Procedurze PR-03 QBP-001/S Nadzór nad dokumentami i zapisami oraz Instrukcji Kancelaryjnej.

4.2 Uwarunkowania klasyfikacji informacji

Klasyfikacja informacji powinna być przeprowadzana przy uwzględnieniu następujących wymagań, zaleceń i uwarunkowań:

1. Informacje mają różne stopnie wrażliwości oraz krytyczności. Klasyfikacja powinna być prowadzona pod kątem znaczenia informacji dla biznesu Szpitala.
2. Klasyfikacja informacji nie zastępuje wymagań prawnych, a jedynie je uzupełnia i dostosowuje do specyfiki działania Szpitala.
3. Wprowadzenie klasyfikacji informacji nie służy rozwiązaniu wszystkich problemów związanych z postępowaniem z informacją i jej ochroną. Ma na celu zapewnienie minimalnych koniecznych do stosowania zabezpieczeń. Nie ogranicza również stosowania dodatkowego poziomu ochrony lub specjalnego traktowania niektórych informacji, które mogą takich zabezpieczeń wymagać.
4. Klasyfikacja informacji musi zapewniać skuteczność i efektywność jej stosowania, czyli:
   a) nie może zawierać zbyt wielu kategorii klasyfikacji,
   b) kryteria klasyfikacji muszą być jednoznaczne i umożliwiać łatwe przyporządkowanie informacji do określonej kategorii,
   c) musi uzupełniać, a nie zastępować wymagania prawne,
   d) musi stosować unikalne nazwy, tak aby unikać przypadkowych pomyłek z klasyfikacjami ustanowionymi w trybie ustawowym,
   e) stosowanie klasyfikacji w jasny sposób musi informować pracowników jak postępować z poszczególnymi informacjami.

4.3 Zasady klasyfikacji informacji

Klasyfikacja informacji oraz dokumentów zawierających te informacje przeprowadzana jest w oparciu o wartość, jaką ta informacja/dokument stanowi dla Szpitala oraz na podstawie wymagań w zakresie poufności wynikających z obowiązujących aktów prawnych.

W Szpitalu przyjęto następujący podział informacji:

- ✓ **Informacje poufne** – sygnatury dla dokumentów **„poufne"** - dostęp do informacji lub dokumentu jest ograniczony do wybranej grupy pracowników Szpitala. Dostęp ten powinien być realizowany zgodnie z zatwierdzoną formalnie listą dostępu. Za opracowanie listy dostępu odpowiedzialny jest właściciel informacji czyli osoba do której dokument jest skierowany lub na kogo jest on zadekretowany. Lista dostępu dla informacji/dokumentu może wskazywać imiennie osoby. Dokumenty tak oznaczone należy przekazywać tylko do osób, które figurują na liście dostępu. W przypadku wskazania sygnatury komórki organizacyjnej, domyślną listą dostępu są pracownicy zatrudnieni w danej komórce. Udostępnienie dokumentu osobom nieupoważnionym wymaga formalnej zgody właściciela informacji lub kierownika komórki organizacyjnej, w której dokument jest przechowywany. Informacje i dokumenty klasyfikowane jako „poufne" powinny znajdować się w obszarach bezpiecznych.
- ✓ **Informacje medyczne (o stanie zdrowia pacjenta)** – dla dokumentów tego typu nie stosuje się listy dostępu, domyślna listą dostępu jest personel Szpitala biorący udział w udzielaniu świadczeń medycznych danego pacjenta. Informacje o stanie zdrowia pacjenta są informacjami o charakterze poufnym. Dokument może być udostępniony tylko osobom, które są do tego upoważnione.
- ✓ **Informacje „do użytku wewnętrznego"** – *sygnatura dla dokumentów* ***„do użytku wewnętrznego"*** *lub* ***„wewnętrzne"*** - do tej grupy kwalifikowane są informacje o istotnym znaczeniu dla funkcjonowania Szpitala - obowiązujące procedury, zarządzenia, materiały szkoleniowe, okólniki, raporty, kontrakty i porozumienia z podmiotami zewnętrznymi, wewnętrzne listy mailingowe i książki telefoniczne, dokumentacje projektowe i wykonawcze, dokumenty wymieniane z innymi podmiotami. Dostęp do nich powinny mieć jedynie osoby pozostające w związku prawnym ze Szpitalem (np. w stosunku zatrudnienia). Udostępnienie tych informacji osobom, podmiotom, które nie pozostają w takim związku wymaga formalnej zgody osób zarządzających Szpitalem. Należy pamiętać, że ewentualne ujawnienie lub przejęcie informacji należących do tej grupy przez osoby nieuprawnione nie może skutkować ryzykiem poważnego zakłócenia funkcjonowania Szpitala. Udostępnienie dokumentu podmiotom zewnętrznym wymaga zgody właściciela informacji.
- ✓ **Informacje ogólnodostępne (publiczne)** – *sygnatura dla dokumentów* ***„publiczne"*** *lub* ***„jawne"***– utrata okresowej dostępności lub ujawnienie informacji tego rodzaju nie stanowi zagrożenia dla ciągłości działania Szpitala. Informacja lub dokument mogą być udostępnione podmiotom zewnętrznym lub osobom spoza Szpitala i nie podlega żadnym ograniczeniom wynikającym z wewnętrznych regulacji. Mogą jednak podlegać ograniczeniom wynikającym z powszechnie obowiązujących przepisów prawa (np. prawa autorskie). Należy pamiętać, że dla niektórych dokumentów ważne jest zachowanie ich integralności i dostępności (np. akty prawne, dokumentacja zamówień publicznych).

Dokumenty zawierające informacje o stanie zdrowia pacjenta nie muszą być oznaczone sygnaturą „poufne" ponieważ wszystkie muszą być chronione przed dostępem osób nieuprawnionych. Dokumenty **„do użytku wewnętrznego"** oraz **„poufne"** muszą być oznaczone sygnaturą. Dokument nie oznaczony według klasyfikacji informacji należy traktować jako dokument do publicznie dostępny z wyłączeniem dokumentów w

oczywisty sposób prawnie chronionych, np. dokumentacja medyczna lub dokumenty zawierające informacje o danych osobowych pacjenta (również o stanie zdrowia).

Sygnatura określająca klasyfikację dokumentu powinna być czytelna umieszczona co najmniej na pierwszej stronie (np. w stopce lub nagłówku dokumentu). Szczegółowy podział dokumentów ze względu na zawartą w nich treść oraz zasady postępowania z tymi dokumentami zostały określone w Załączniku nr 4 do niniejszego dokumentu. Dokumenty należy umieszczać w odpowiednio oznaczonej szafie, segregatorze lub w miejscu określonym dla danego rodzaju dokumentów i ich klas. Jeżeli wszystkie miejsca w pomieszczeniu, w których przechowuje się dokumenty zawierają lub mogą zawierać dokumenty sklasyfikowane jako „poufne" oznakowanie tych miejsc nie jest wymagane. Dostęp do informacji i dokumentów klasyfikowanych jako poufne realizowany jest zgodnie z zatwierdzoną formalnie listą dostępu. Za opracowanie i utrzymywanie aktualnej listy dostępu odpowiedzialny jest właściciel informacji klasyfikowanej jako „poufne".

Właściciel informacji w systemie SZBI określa osobę odpowiedzialną za zarządzanie tą informacją. Jest to zazwyczaj komórka organizacyjna, w której informacja powstała lub osoba, która otrzymała takie uprawnienia.

Dokumenty zawierające dane osobowe (np. akta pracownicze, dokumentacja medyczna) są dokumentami chronionymi i należy z nimi postępować jak w przypadku dokumentów sklasyfikowanych jako „poufne". Ze względu na trudności utworzenia imiennych list w takich wypadkach dopuszcza się tzw. domyślne listy dostępu. Wszyscy pracownicy muszą posiać upoważnienia do przetwarzania danych osobowych. Dopuszczenie do przetwarzania danych osobowych pracownika odbywa się na zasadach określonych w Procedurze PR-04 QBP-02 System kontroli dostępu.

Dla dokumentacji medycznej nie tworzy się listy dostępu. Domyślną listą dostępu jest personel medyczny udzielający świadczeń (m.in. lekarze, pielęgniarki), pracownicy niemedyczni (np. sekretarki medyczne, pracownicy rejestracji, technicy wykonujący badania lub opisy), którzy mają kontakt z tą dokumentacją w trakcie realizacji powierzonych im zadań.

Dla informacji zawierających dane osobowe pracowników domyślną listą dostępu jest lista pracowników zatrudnionych w Dziale Spraw Pracowniczych i posiadających stosowne upoważnienie do przetwarzania tych danych.

Dla wszystkich informacji przetwarzanych przez system informatyczny w Szpitalu domyślną listą dostępu stanowią pracownicy Działu Informatyki. W zakresie niezbędnym do realizacji przydzielonych im zadań nadzorowania i administrowania systemem informatycznym posiadają oni dostęp m.in. do danych osobowych (w tym również danych wrażliwych) oraz wszystkich innych informacji przetwarzanych przez system informatyczny Szpitala.

W Szpitalu mogą występować także informacje i dokumenty niejawne, przetwarzane zgodnie z przepisami o ochronie informacji niejawnej, czego nie obejmuje niniejsza polityka.

W trakcie przeprowadzanych kontroli, auditów osoby posiadające stosowne upoważnienia są do zapoznania się z dokumentacją w zakresie wynikającym z celu kontroli lub auditu.

4.4 Przekazywanie i udostępnianie informacji

Zaleca się by przekazywanie informacji o charakterze poufnym (np. dane osobowe, informacje o stanie zdrowia) odbywało się z zachowaniem należytych środków ochrony. Wymiana informacji może być realizowana za pomocą wielu środków komunikacji różnego typu, łącznie z pocztą elektroniczną, nośnikami typu pendrive, głosem, faksem oraz wideo. W przypadku przekazywania informacji głosem należy pamiętać że rozmowa może zostać podsłuchana. Z tego powodu nie należy prowadzić rozmów o charakterze poufnym na korytarzach, w miejscach ogólnie dostępnych. Zasady wykorzystywania poczty elektronicznej do przekazywania informacji o charakterze poufnym opisano w Rozdziale 7.8 niniejszego dokumentu oraz Regulaminie użytkownika systemu informatycznego – Załącznik nr 7 do niniejszego dokumentu. Zakazane jest przesyłanie dokumentów o charakterze poufnym (np. zawierającym dane osobowe) przy pomocy faxu.

Za udostępnianie informacji rozumieć m.in.:

- ✓ przekazanie informacji lub nośnika z danymi
- ✓ weryfikację danych,
- ✓ powierzenie danych,
- ✓ umożliwienie wglądu,
- ✓ upublicznienie.

Formalnym warunkiem udostępnienia danych osobowych jest udostępnianie informacji w trybie szczególnego przepisu prawa. Wniosek o udostępnienie danych musi zawierać: podstawę prawną, cel udostępnienia, zakres żądanych informacji, do kogo jest kierowany, imię i nazwisko wnioskującego oraz podpis. Wyjątek stanowi zapytanie o dostęp do informacji publicznej, w którym nie jest wymagane określenie celu. W odpowiedzi na wniosek o dostęp do informacji publicznej udziela się informacji w przedmiotowym zakresie ale bez danych osobowych zawartych w tych dokumentach. Zastrzeżenie nie dotyczy informacji o funkcjonariuszach publicznych.

W przypadku transportowania nośników informacji należy chronić nośniki przed uszkodzeniem fizycznym poprzez odpowiednie przechowywanie i pakowanie. Należy pamiętać o zabezpieczeniu ich przed szkodliwym wpływem czynników środowiskowych tj. temperatura, wilgotność , pole magnetyczne.

W przypadku transportu nośników dowolnego typu (np. papier, płyta DVD) zawierających dane o charakterze poufnym należy:

- ✓ pakować je w sposób ujawniający próbę otwarcia,
- ✓ przesyłkę dostarczyć do rąk własnych,
- ✓ korzystać z zaufanego transportu lub kurierów.

Zaleca się by w umowach z podmiotami zewnętrznymi, z którymi następuje wymiana informacji o charakterze poufnym, drogą inną niż elektroniczna, były wskazane z imienia i nazwiska osoby odpowiedzialne za korespondencję. Przesyłki tego typu muszą być adresowane imiennie na osoby upoważnione.

4.4.1 Udostępnianie dokumentacji medycznej oraz informacji o stanie zdrowia.

Wymagania prawne dotyczące zasady udzielania informacji o stanie zdrowia pacjenta oraz dokumentacji medycznej określone zostały w normatywnych aktach prawnych wskazanych na stronie wewnętrznej Szpitala. Szczegółowy tryb postępowania w tym zakresie obowiązujący pracowników Szpitala unormowany został w odrębnym dokumencie – Zarządzeniu Dyrektora w sprawie zasad i trybu udostępniania dokumentacji medycznej, udzielania informacji zakładom ubezpieczeń, wydawania orzeczeń, opinii i zaświadczeń oraz opłat za udostępnianie dokumentacji medycznej. Informacji o stanie zdrowia pacjenta może udzielać lekarz prowadzący lub ordynator/kierownik oddziału osobie upoważnionej zgodnie z obowiązującymi w tym zakresie przepisami. Należy pamiętać, że z powodu braku możliwości identyfikacji rozmówcy nie należy udzielać informacji o stanie zdrowia pacjenta przez telefon lub faxem.

4.4.2 Udzielanie informacji o danych osobowych osób zatrudnionych

Informacje o osobach zatrudnionych (dane osobowe, wysokość wynagrodzenia, informacje o najbliższych) podlegają ochronie na podstawie ustawy o ochronie danych osobowych. Udzielenie informacji w tym zakresie udziela się tylko podmiotom uprawnionym w tym zakresie na podstawie formalnego wniosku.

Nie należy udostępniać jakichkolwiek informacji o danych osobowych pracowników osobom nieupoważnionym. W szczególności nie należy podawać takich informacji telefonicznie m.in. o miejscu zamieszkania, wysokości zarobków, obecności lub absencji w pracy. W odniesieniu do lekarzy przyjmujących w poradniach i przychodniach można udzielić informację tylko w zakresie planowanych terminów wizyt. W pozostałych sytuacjach nie należy udzielać informacji o obecności lub absencji. Niedopuszczalne jest informowanie o powodach absencji.

4.4.3 Udostępnianie informacji i dokumentacji dotyczącej finansowania zadań ze środków publicznych.

Szpital jest jednostką należącą do sektora finansów publicznych. Dokumenty dotyczące finansowania zadań ze środków publicznych nie mają charakteru zastrzeżonego z wyłączeniem m.in.: informacji technicznych, technologicznych, organizacyjnych lub gdy informacja stanowi tajemnicę Szpitala z uwagi na istotny interes publiczny lub ważny interes państwa. Każdy obywatel ma prawo do uzyskania informacji w zakresie zasad finansowania Szpitala. Prawo do informacji publicznej podlega ograniczeniu w zakresie i na zasadach określonych w przepisach o ochronie informacji niejawnych oraz o ochronie innych tajemnic ustawowo chronionych, jak również ze względu na prywatność osoby fizycznej lub tajemnicę przedsiębiorcy. Osobą odpowiedzialną za udzielenie informacji w zakresie finasowania realizowanych przez Szpital zadań ze środków publicznych jest Główny Księgowy lub osoba przez niego upoważniona. Udzielenie odpowiedzi w przedmiotowej sprawie wymaga złożenia przez zainteresowaną stronę stosownego wniosku z zachowaniem formy pisemnej.

4.4.4 Kontakt z podmiotami zewnętrznymi

Każdy pracownik Szpitala może udzielać informacji mediom w zakresie i na zasadach określonych w stosownym Zarządzeniu Dyrektora. Do udzielania informacji na zewnątrz w sprawach dotyczących działalności Szpitala upoważnieni są: Dyrektor i jego zastępcy w sprawach wynikających z działalności nadzorowanego pionu oraz Rzecznik Prasowy. Pracownicy Szpitala mogą udzielać informacji na zewnątrz w zakresie przydzielonych im do załatwienia spraw, wyłącznie po uzyskaniu zgody Dyrektora Szpitala, pod warunkiem nienaruszenia przepisów o zachowaniu poufności, w szczególności tajemnicy pracodawcy oraz przewidzianej przepisami ustaw o ochronie informacji niejawnych, o ochronie danych osobowych oraz dostępie do informacji publicznej i o ile udzielona informacja nie przyniesie szkody interesom Szpitala.

5. Bezpieczeństwo osobowe

Jednym z głównych celów bezpieczeństwa osobowego jest zapewnienie odpowiedniej świadomości i kompetencji personelu mającego wpływ na bezpieczeństwo. Cel ten jest realizowany nie tylko przez szkolenia i podnoszenie świadomości pracowników, ale także poprzez działania podczas zatrudnienia, zmiany zatrudnienia lub jego zakończenia. Działania te mają głównie na celu ograniczenie ryzyka błędu ludzkiego, niewłaściwego użytkowania zasobów czy też nieodpowiedniego postępowania z informacją.

Na bezpieczeństwo osobowe duży wpływ ma poprawne zdefiniowanie ról i zakresów odpowiedzialności wszystkich pracowników Szpitala mających wpływ na bezpieczeństwo informacji. Role i zakresy odpowiedzialności w obszarze bezpieczeństwa informacji są określone w sposób formalny. Opis ról i zakresów odpowiedzialności w tym obszarze uwzględnia i definiuje:

- ✓ działania podejmowane przez pracownika w ramach procesu bezpieczeństwa,
- ✓ odpowiedzialności osoby za jej działania,
- ✓ sposoby ochrony zasobów i informacji, do których pracownik ma dostęp, przed nieuprawnionym dostępem, ujawnieniem, modyfikacją, zniszczeniem lub zniekształceniem,
- ✓ ewentualne sposoby raportowania zdarzeń związanych lub potencjalnie związanych z bezpieczeństwem informacji.

Zgodnie z obowiązująca w Szpitalu Procedurą PR-04 QBP-01, obowiązki oraz odpowiedzialność pracownika na stanowisku pracy są mu zakomunikowane przed rozpoczęciem pracy. Pracownik poświadcza pisemnie przyjęcie Zakresu zadań, obowiązków i uprawnień. Dokument ten przechowuje się w aktach pracowniczych. Lekarze zatrudnieni w trybie art. 26 i 26a zakres zadań i odpowiedzialności mają określony w stosownej umowie.

5.1 Rozpoczęcie, zamiana i zakończenie zatrudnienia

Zatrudnienie i zmiana zatrudnienia pracownika powinno odbywać się na zasadach jawności, otwartości i konkurencyjności postępowania. Postępowanie podczas naboru lub zmiany stanowiska pracy pracownika odbywa się zgodnie z obowiązującą Procedurą PR-04 QBP-01. Każdy pracownik zapoznaje się z powierzonymi mu obowiązkami określonymi w „Zakresie zadań, uprawnień i odpowiedzialności". Ustanie zatrudnienia pracownika odbywa się z uwzględnieniem wymagań w zakresie bezpieczeństwa informacji.

5.2 Ogólne zasady bezpieczeństwa osobowego

Każdy pracownik przy wykonywaniu swoich obowiązków służbowych jest zobowiązany do przestrzegania postanowień niniejszej polityki oraz postanowień innych części dokumentacji bezpieczeństwa informacji, a także poleceń dotyczących bezpieczeństwa otrzymywanych od przełożonych, przedstawicieli Komitetu Bezpieczeństwa, właścicieli zasobów, systemów i dokumentów. W razie wątpliwości, co do obowiązujących zasad postępowania dotyczących bezpieczeństwa, dokumentacji bezpieczeństwa informacji oraz użytkowania zabezpieczeń pracownik jest zobowiązany zwrócić się o pomoc do swojego przełożonego. W przypadku braku możliwości rozwiązania problemu przełożony może zwrócić się o pomoc w przedmiotowej sprawie do Komitetu ds. Bezpieczeństwa.

Każdy z pracowników jest zobowiązany do uczestniczenia w organizowanych w Szpitalu okresowo szkoleniach z zakresu bezpieczeństwa informacji.

Każdy pracownik jest zobowiązany do podjęcia bezpośrednich działań dla zapobiegania incydentom lub minimalizowania skutków incydentów w miarę swoich możliwości i kompetencji, w razie potrzeby zawiadamiając przełożonych, odpowiednie służby ratownicze, przedstawiciela Komitetu ds. Bezpieczeństwa. O zgłoszeniu incydentu bezpieczeństwa do policji decyduje osoba upoważniona przez Dyrektora. W przypadku popełnienia czynu zabronionego każda osoba jest uprawniona do zgłoszenie tego faktu policji.

5.3 Ogólne zasady przyznawania dostępu

Ze względu na konieczność ochrony przechowywanych dokumentów oraz przetwarzanych informacji o różnorakiej klasyfikacji wprowadza się odpowiednie zabezpieczenia. Szczegóły dotyczące stosowanych zabezpieczeń oraz sposobu zarządzania przywilejami w zakresie dostępu do stref bezpieczeństwa i systemów informatycznych zawarte są w Procedurze PR-04 QBP-02 System kontroli dostępu. Przyznawanie zakresu uprawnień dostępu do poszczególnych stref oraz zasobów odbywa się w ścisłym związku z zakresem obowiązków danego pracownika. Zarządzanie dostępem do stref bezpieczeństwa, informacji, dokumentów, środków przetwarzania informacji realizowane jest w oparciu o potrzeby biznesowe i wymagania bezpieczeństwa.

5.4 Zarządzanie dostępem zdalnym

Udzielanie i cofanie pracownikom lub podmiotom zewnętrznym dostępu zdalnego do zasobów informatycznych Szpitala odbywa się zgodnie z Procedurami PR-05 QBP-02/E Nadzór nad sprzętem komputerowym i oprogramowaniem oraz PR-05 QBP-03/E Uruchamianie systemu i odtwarzanie danych.

5.5 Sankcje porządkowe, dyscyplinarne i karne

Naruszenie lub przyczynienie się (umyślne lub nieumyślne) do naruszenia postanowień Polityki Bezpieczeństwa Informacji przez pracownika, niezastosowanie się do poleceń służbowych w tym zakresie, powinno być potraktowane jako naruszenie obowiązków służbowych. W takiej sytuacji pracownik może zostać:

- ✓ ukarany zgodnie z obowiązującym w Szpitalu Regulaminem Pracy,
- ✓ ukarany grzywną przez organy do tego upoważnione w wysokości przewidzianej przepisami prawa,
- ✓ pociągnięty do odpowiedzialności karnej.

Z wnioskiem o wyciągnięcie konsekwencji względem pracownika, który naruszył obowiązujące zasady bezpieczeństwa może wystąpić przełożony pracownika, Kierownik Pionu Organizacji i Systemów Zarządzania,

Pełnomocnik ds. Bezpieczeństwa lub Administrator Bezpieczeństwa. Ostateczną decyzję w tym zakresie podejmuje Dyrektor.

6. Bezpieczeństwo fizyczne

Celem podstawowym w zakresie zapewnienia bezpieczeństwa fizycznego jest zabezpieczenie infrastruktury, pomieszczeń i wyposażenia przed nieuprawnionym dostępem, zakłóceniem funkcjonowania bądź uszkodzeniem. Kluczowym jest bezpieczeństwo obszarów, w których przetwarzana jest informacja lub dokumenty o klasie „do użytku wewnętrznego" lub „poufne" oraz obszarów, w których znajduje się wyposażenie przetwarzające te informacje lub dokumenty oraz pomieszczenia, w których przebywanie z innych względów powinno odbywać się pod nadzorem. System bezpieczeństwa fizycznego opiera się na następujących wymaganiach i zasadach:

- ✓ Szpital jest podzielony na strefy bezpieczeństwa wykorzystujące system kontroli dostępu,
- ✓ dostęp do wybranych stref bezpieczeństwa jest ograniczony zgodnie z zasadą dostępu minimalnego, niezbędnego do realizacji zadań służbowych,
- ✓ dostęp do szczególnie chronionych stref bezpieczeństwa jest rejestrowany,
- ✓ obowiązuje kategoryczny zakaz dostępu osób nieuprawnionych do obszarów chronionych Szpitala bez nadzoru osoby do tego uprawnionej,
- ✓ przyjęcie przez wszystkich pracowników do realizacji reguł postępowania w strefach bezpieczeństwa zgodnych z niniejszym dokumentem.

6.1 Podział obiektu na strefy

Szpital zgodnie z wymaganiami bezpieczeństwa posiada wydzielone następujące strefy bezpieczeństwa:

- ✓ strefa publicznie dostępna – strefa bez ograniczenia dostępu – strefa ta obejmuje korytarze, poczekalnię, sale chorych, korytarze oddziałów, osoby przebywające w strefie nie podlegają rejestracji.
- ✓ strefa administracyjna – osoby przebywające w strefie nie podlegają rejestracji. Poszczególne pomieszczenia w strefie administracyjnej należy traktować jako strefy ograniczonego dostępu. Dla poszczególnych pokoi prowadzony jest rejestr praw dostępu.
- ✓ strefa ograniczonego dostępu – obszar, w którym obowiązują zasady ograniczenia dostępu (np. określone pory dnia lub tygodnia) bazujące na zabezpieczeniach organizacyjnych. Osoba nie zatrudniona w danej strefie, (np. pacjent, inny pracownik) przebywa tam tylko w obecności upoważnionego pracownika. W strefie obowiązuje system kontroli dostępu - stosowne są zabezpieczenia w postaci zamków a dostęp do kluczy (kodów, elektronicznych kart dostępu) podlega rejestracji . Osoby przebywające w strefie nie podlegają rejestracji.
- ✓ strefa chroniona – strefa dostępna jedynie dla wybranego personelu (medycznego i/lub pracowników służb technicznych, innych). W tej strefie obowiązuje system kontroli dostępu. Wszystkie osoby przebywające w tej strefie podlegają rejestracji (z wyłączeniem osób upoważnionych oraz pacjentów, którym udzielane są świadczenia medyczne), ich przebywanie musi zostać odnotowane w karcie strefy chronionej. Sprzątanie odbywa się tylko w obecności pracownika posiadającego upoważnienie do dostęp do pomieszczeń.

Administrator Bezpieczeństwa Fizycznego i Osobowego w porozumieniu z Pełnomocnikiem ds. Bezpieczeństwa odpowiedzialny jest za opracowanie:

- ✓ podziału obszaru Szpitala na obszary bezpieczne,
- ✓ wdrożenie i zarządzanie systemem kontroli dostępu do stref bezpieczeństwa,
- ✓ autoryzacji nadawania i cofania uprawnień do stref bezpieczeństwa.

6.2 Podstawowe obowiązki pracowników w fizycznych strefach bezpieczeństwa

Niniejsza Polityka nie obejmuje zasad bezpieczeństwa pracy w obszarach bezpiecznych. Zasady bezpiecznej pracy w strefach powinny odpowiadać wszystkim strefom bezpieczeństwa wyróżnionym w planie stref bezpiecznych.

Wszyscy pracownicy Szpitala odpowiedzialni są za przestrzeganie poniższych ogólnych wymagań bezpieczeństwa:

- ✓ każdy pracownik odpowiada osobiście za bezpieczeństwo swego miejsca pracy w momencie jego opuszczenia,
- ✓ każdy pracownik jest zobowiązany do stosowania zasady czystego biurka – po opuszczeniu stanowiska pracy dokumenty chronione powinny być zabezpieczone przed nieuprawnionym dostępem,
- ✓ każdy pracownik jest zobowiązany do stosowania zasady czystego ekranu – po opuszczeniu stanowiska pracy przez pracownika nie powinny być wyświetlane na monitorze komputera informacje chronione,
- ✓ dostęp wszystkich pracowników jest ograniczony jedynie do stref i pomieszczeń oraz miejsc pracy niezbędnych w realizacji powierzonych im działań,
- ✓ zabronione jest wpuszczanie do stref bezpieczeństwa wykorzystującej indywidualny system kontroli dostępu osób nieuprawnionych bez nadzoru,
- ✓ dostęp do stref i pomieszczeń jest zabezpieczony ogólnym systemem ochronnym (np. klucze) oraz indywidualnymi środkami ochrony (np. hasła lub kody dostępowe, karty elektroniczne),
- ✓ zakazane jest podejmowanie prób samodzielnej naprawy lub modyfikacji instalacji i urządzeń mających wpływ na bezpieczeństwo przez nieupoważnione osoby,

- ✓ osoby spoza Szpitala wykonujące prace porządkowe, instalacyjne, konserwacyjne muszą być nadzorowane w strefie chronionej przez pracownika wyznaczonego przez kierownika komórki organizacyjnej (do którego należą pomieszczenia, w których te czynności są prowadzone), a pod jego nieobecność Administratora Bezpieczeństwa Fizycznego i Osobowego lub Pełnomocnika ds. Bezpieczeństwa.

6.3 Podstawowe zasady bezpieczeństwa dotyczące kluczy, kart dostępu, kodów i identyfikatorów

Pracownicy, którym przydzielono klucze, kody lub identyfikatory (w tym w formie elektronicznych kart dostępu) zobowiązani są do ich bezpiecznego przechowywania tak, aby ograniczyć dostęp osób nieupoważnionych. Nie jest dozwolone udostępnianie lub przekazywanie przydzielonych identyfikatorów, kluczy, kodów innym nieupoważnionym pracownikom lub innym osobom bez pisemnej zgody kierownika komórki organizacyjnej, Administratora Bezpieczeństwa Fizycznego i Osobowego lub Pełnomocnika ds. Bezpieczeństwa. Zakazane jest wykonywanie duplikatów przydzielonych kluczy bez zgody Administratora Bezpieczeństwa Fizycznego i Osobowego. Na żądanie kierownika komórki organizacyjnej, Administratora Bezpieczeństwa Fizycznego lub Pełnomocnika ds. Bezpieczeństwa wymagane jest okazanie lub zwrócenie przydzielonych kluczy. W przypadku utraty przydzielonych kluczy wymagane jest niezwłoczne powiadomienie o tym fakcie kierownika komórki organizacyjnej oraz Administratora Bezpieczeństwa Fizycznego i Osobowego.

Administrator Bezpieczeństwa Fizycznego i Osobowego jest odpowiedzialny za prowadzenie i aktualizację planu praw dostępu do stref bezpieczeństwa dla których klucze są przekazywane do posterunków ochrony. Dla pomieszczeń, w których praca odbywa się w cyklu zmianowym a klucze nie są zdawane na posterunek ochrony dopuszcza się prowadzenie odrębnego rejestru praw dostępu. Dla pomieszczeń wykorzystywanych przez personel medyczny dopuszcza się rejestr osób uprawnionych w postaci domyślnej. Osobami upoważnionymi jest grupa personelu medycznego realizująca swoje zadania w określonych pomieszczeniach np. dla pokoju lekarskiego domyślnym grupą osób uprawnionych stanowią lekarze zatrudnieni w danym oddziale, punkt pielęgniarski – domyślną grupę osób zatrudnionych stanowią pielęgniarki zatrudnione na danym oddziale.

Wprowadzony zostaje obowiązek zamykania pomieszczeń znajdujących się w budynkach Szpitala z wykorzystaniem dostępnych zabezpieczeń.

Celem podstawowym wymaganym od każdego pracownika w zakresie zapewnienia bezpieczeństwa informacji jest uświadomienie wszystkim zainteresowanym, że:

- ✓ dostęp wszystkich pracowników jest ograniczony jedynie do stref i pomieszczeń oraz miejsc pracy niezbędnych w realizacji powierzonych im działań (poza strefami publicznie dostępnymi),
- ✓ dostęp do stref i pomieszczeń jest zabezpieczony ogólnym systemem ochronnym (np. klucze) oraz indywidualnymi środkami ochrony (np. hasła lub kody dostępowe, karty elektroniczne),
- ✓ każdy z użytkowników odpowiada osobiście za bezpieczeństwo swego miejsca pracy w momencie jego opuszczenia (czysty ekran, czyste biurko, pomieszczenie zamknięte i zabezpieczone zgodnie z obowiązującymi wymaganiami w poszczególnych strefach).

Incydenty i zakłócenia z tego tytułu traktowane będą jako naruszenia zasad bezpieczeństwa informacji ze wszystkimi tego konsekwencjami służbowymi i prawnymi.

Dostęp do stanowisk pracy i stacji roboczych, przy zachowaniu maksymalnie korzystnych warunków ochrony i eksploatacji sprzętu przez uprawnionych użytkowników realizowany jest przez:

- ✓ system kontroli dostępu w wyszczególnionych lokalizacjach,
- ✓ ograniczony dostęp do wybranych stref,
- ✓ kategoryczny zakaz dostępu osób nieuprawnionych do pomieszczeń chronionych mechanicznie (np. zamki szyfrowe, kłódki szyfrowe z równoczesnym plombowaniem) newralgicznych elementów systemów informatycznych (np. szafy krosownicze, skrzynki połączeniowe i przyłącza) i innych wybranych pomieszczeń Szpitala,
- ✓ przyjęcie przez wszystkich pracowników do realizacji reguły ochronnej we wszystkich lokalizacjach, wobec podmiotów zewnętrznych.

Szczegółowe zasady dotyczące zarządzania prawami dostępu zawiera procedura PR-04 QBP-02 System kontroli dostępu.

6.4 Wykaz budynków oraz pomieszczeń, w których przetwarzane są dane osobowe

Z uwagi na wymagania prawne dotyczące nadzoru miejsc, w których przetwarzane są dane osobowe prowadzi się wykaz tego typu pomieszczeń. Osobą odpowiedzialną za sporządzenie i aktualizację wykazu jest ABFiO. W przypadku zaadaptowania pomieszczenia na czynności związane z przetwarzaniem danych osobowych kierownik komórki organizacyjnej niezwłocznie zawiadamia o tym fakcie ABFiO. Niedopełnienie tego wymogu stanowić będzie naruszenie zasad bezpieczeństwa.

7. Bezpieczeństwo teleinformatyczne

Jednym z najważniejszych aspektów zapewnienia bezpieczeństwa informacji jest sprawne zarządzanie zasobami przetwarzającymi informacje. Wykorzystywane zasoby mogą mieć znaczny wpływ na funkcjonowanie procesów biznesowych i dlatego ważne jest zapewnienie bezpieczeństwa od początku cyklu życia zasobu aż do jego zakończenia. Przedstawione w niniejszym rozdziale zasady bezpieczeństwa teleinformatycznego dotyczą określenia wymagań zasobu, autoryzacji, konfiguracji, monitorowania, nadawania dostępu, zbywania oraz utylizacji najważniejszych zasobów. Przy ochronie zasobów – nie tylko ujętych w dalszej części niniejszej polityki – kluczowe jest stosowanie podstawowej zasady bezpieczeństwa, że nie jest dozwolone wykorzystywanie zasobów w sposób inny niż jawnie dozwolony.

Szczegółowe zasady pracy z wykorzystaniem systemów, sprzętu i oprogramowania informatycznego w Szpitalu (opisane w procedurze) określa i wdraża Dział Informatyki w koordynacji z Pełnomocnikiem ds. Bezpieczeństwa oraz ABFiO. Od tej reguły mogą być przewidziane odstępstwa wynikające ze specyfiki pracy komórek organizacyjnych Szpitala, zgodnie z wymogami ustaw i rozporządzeń zaakceptowane przez ABT lub Pełnomocnika ds. Bezpieczeństwa. Podstawowe zasady bezpieczeństwa dla użytkowników systemów teleinformatycznych określono w Regulaminie użytkownika systemu informatycznego – Załącznik nr 7 do niniejszego dokumentu.

7.1 Autoryzacja i dopuszczalne wykorzystanie zasobów

Do wykonywania obowiązków służbowych związanych z przetwarzaniem informacji dozwolone jest używanie systemów, urządzeń i oprogramowania dopuszczonych do użytku zgodnie z wymogami Polityki Bezpieczeństwa Informacji.

Pracownicy są uprawnieni do korzystania z zasobów teleinformatycznych Szpitala niezbędnych do wykonywania swoich obowiązków. Za określenie takich zasobów dla każdego pracownika Szpitala i wnioskowanie o przyznanie dostępu odpowiedzialny jest kierownik komórki organizacyjnej pracownika. Szczegółowe zasady nadawaniu uprawnień opisano w procedurze PR-04 QBP-02 System kontroli dostępu.

Zakazane jest użytkowanie na terenie Szpitala lub przy wykonywaniu obowiązków służbowych poza Szpitalem innych niż dopuszczone urządzeń, systemów i oprogramowania bez zgody Administratora Bezpieczeństwa Teleinformatycznego lub Pełnomocnika ds. Bezpieczeństwa.

Zakazane jest bez pisemnej zgody Administratora Bezpieczeństwa Teleinformatycznego:

- ✓ użytkowanie urządzeń skutkujących połączeniem systemów Szpitala z sieciami teleinformatycznymi innych podmiotów, w tym publicznymi sieciami teleinformatycznymi,
- ✓ użytkowanie urządzeń lub oprogramowania mających na celu zakłócenie działania innych systemów, urządzeń lub oprogramowania,
- ✓ użytkowanie urządzeń lub oprogramowania do testowania bezpieczeństwa lub wykrywania podatności,
- ✓ użytkowanie urządzeń lub oprogramowania mogących naruszyć bezpieczeństwo innych systemów lub urządzeń,
- ✓ użytkowanie innych urządzeń lub oprogramowania stwarzających zagrożenie – według najlepszej wiedzy pracownika i przy zachowaniu niezbędnej ostrożności – dla bezpieczeństwa informacji lub zasobów lub środowiska pracy,
- ✓ wprowadzanie zmian konfiguracji urządzeń, systemów lub oprogramowania.

Dopuszcza się odstępstwo od powyższych zasad w sieciach testowych wyróżnionych i opisanych w schemacie sieci LAN/WAN stanowiącym część Szczegółowej Polityki Bezpieczeństwa Informacji.

Ograniczenia w korzystaniu z pewnych aktywów (zasobów lub informacji) mogą być nałożone przez gestorów tych aktywów – w takim przypadku gestor aktywu zobowiązany są do poinformowania o charakterze ograniczenia i terminie jego obowiązywania tych pracowników, których to ograniczenie dotyczy oraz prowadzenia formalnej dokumentacji tego ograniczenia.

Wykorzystanie należących do Szpitala urządzeń, systemów i oprogramowania oraz innych zasobów do prywatnych celów pracowników jest dozwolone jedynie na uzasadniony wniosek kierownika komórki organizacyjnej pracownika i za zgodą Administratora Bezpieczeństwa Teleinformatycznego. Dozwolone jest korzystanie do celów prywatnych z dostępu do Internetu, kont poczty elektronicznej, telefonów komórkowych oraz pamięci USB w sposób niepowodujący powstania po stronie Szpitala nadmiernych kosztów związanych z wykorzystywanym zasobem oraz przeciążeniem sieci. Szpital zastrzega sobie prawo do monitorowania wykorzystywania tych zasobów przez pracowników oraz do cofnięcia w dowolnej chwili takiej zgody. **Rozpoczęcie korzystania z tak udostępnionych zasobów do celów prywatnych (internet, poczta prywatna) przez pracownika jest równoznaczne z wyrażeniem przez niego zgody na monitorowanie przez Szpitala sposobu ich wykorzystania, w tym możliwości wglądu w przetwarzane przez pracownika dane (również korespondencję) oraz zgody na udostępnianie wglądu, zwrotu lub zaprzestania wykorzystywania zasobu na żądanie Administratora Systemu, Administratora Bezpieczeństwa Teleinformatycznego lub Pełnomocnika ds. Bezpieczeństwa.**

Wykorzystanie zasobów Szpitala do celów prywatnych nie zwalnia z obowiązku przestrzegania zasad postępowania z tymi zasobami określonymi w Polityce Bezpieczeństwa Informacji.

Zakazane jest wykorzystanie zasobów Szpitala do celów sprzecznych z obowiązującymi przepisami prawa, również wtedy, gdy są one udostępnione do wykorzystania dla celów prywatnych.

Dane służące do celów prywatnych, zapisane na systemach, urządzeniach, nośnikach danych i innych zasobach w trakcie korzystania z nich muszą być po zakończeniu korzystania z systemu, urządzenia, nośnika lub innego zasobu usunięte.

Zasoby Szpitala powinny być przechowywane w taki sposób, aby zapobiec możliwości ich kradzieży lub uszkodzenia przez osoby spoza Szpitala oraz przypadkowe uszkodzenia przez osoby lub czynniki środowiskowe.

Wynoszenie aktywów poza Szpital możliwe jest za pisemną zgodą właściciela aktywa lub kierownika komórki organizacyjnej na uzasadniony wniosek zainteresowanego poza przypadkami, gdy jest to ujęte w planie praw dostępu.

Pracownicy zobowiązani są stosować zasadę czystego biurka – wszystkie dokumenty i materiały powinny być po zakończeniu pracy chowane w przeznaczonych do tego szafkach, szufladach itp. W przypadku braku dostatecznej ilości dostępnego miejsca dokumenty i materiały powinny być pozostawiane na biurku w sposób uporządkowany. Ta zasada nie wyłącza obowiązujących zasad postępowania z dokumentami sklasyfikowanymi jako „poufne" oraz informacjami niejawnymi.

Pracownicy zobowiązani są do niezwłocznego odbierania wykonanych wydruków, kopii z urządzeń wielodostępowych tak, aby zapobiec dostępowi do dokumentów osób nieupoważnionych.

Pracownicy są zobowiązani do ochrony zasobów będących własnością innych podmiotów, lecz powierzonych lub oddanych do dyspozycji Szpitala lub udostępnionych pracownikom na czas wykonywania przez nich czynności służbowych w takim samym stopniu jak w przypadku zasobów będących własnością Szpitala.

7.2 Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych

Wykaz zbiorów danych osobowych wraz ze wskazaniem programów stosowanych do przetwarzania danych osobowych oraz sposób przepływu danych pomiędzy systemami został szczegółowo opisany w Załączniku nr 1 do Instrukcji Zarządzania systemem informatycznym przetwarzającym dane osobowe.

7.3 Bezpieczeństwo serwerów, komputerów stacjonarnych i przenośnych

Zasady dotyczące zapewnienia odpowiedniego poziomu bezpieczeństwa informacji przetwarzanej i przechowywanej na serwerach, i pozostałych komputerach Szpitala określone zostały w procedurach systemowych, Regulaminie użytkownika systemu informatycznego - Załącznik nr 7 do niniejszego dokumentu, oraz Instrukcji zarządzania systemem informatycznym przetwarzającym dane osobowe.

7.4 Bezpieczeństwo sieci

Zasady dotyczące zapewnienia bezpieczeństwa związanego z konfiguracją i wykorzystaniem sieci komputerowej Szpitala oraz pracujących w niej aktywnych urządzeń sieciowych służących do przetwarzania informacji określono w Procedurze PR-05 BP-03/E Uruchamianie systemu i odtwarzanie danych.

7.5 Bezpieczeństwo haseł

Identyfikator wraz z hasłem są najważniejszą metodą uwierzytelniania użytkowników w systemach informatycznych. Obowiązki pracownika w zakresie ustanawiania haseł mającego uprawnienia dostępu systemów informatycznych opisano w Regulaminie użytkownika systemu informatycznego stanowiący Załącznik nr 7 do niniejszego dokumentu.

Udostępnienie hasła, karty lub PIN-u jest naruszeniem postanowień niniejszej Polityki i podlega zgłoszeniu jako incydent.

Jeśli zachodzi podejrzenie, że hasło zostało skradzione, złamane lub ujawnione należy bezzwłocznie je zmienić, a o tym fakcie poinformować Administratora Bezpieczeństwa Teleinformatycznego.

Hasła w bazach haseł powinny być przechowywane w postaci zaszyfrowanej. W ramach monitorowania systemu zarządzania bezpieczeństwem informacji zaleca się okresowe (w zaplanowanych odstępach czasu) weryfikowanie siły haseł.

7.6 Bezpieczeństwo oprogramowania

Poniższe zasady dotyczące zapewnienia odpowiedniego poziomu bezpieczeństwa informacji związanego z wykorzystywanym w Szpitalu oprogramowaniem (instalacji oraz użytkowania) określone zostały w procedurach systemowych, Regulaminie użytkownika systemu informatycznego stanowiącym Załącznik nr 7 do niniejszego dokumentu oraz Instrukcji zarządzania systemem informatycznym przetwarzającym dane osobowe.

Szczegółowe zasady bezpieczeństwa dotyczące oprogramowania oraz zapewnienia odpowiedniego poziomu bezpieczeństwa informacji (danych) podczas prac rozwojowych przy oprogramowaniu w Szpitalu (planowania prac, zmian, testowania, instalacji, wdrożenia i monitorowania) określone zostały w Procedurze PR-05 QBP-02/E Nadzór nad sprzętem komputerowym i oprogramowaniem.

7.7 Zapasowe kopie danych

Tworzeniu kopii zapasowych podlegają wszystkie typy informacji oraz urządzenia ujęte w wykazie informacji objętych tworzeniem kopii zapasowych. W szczególności, dla systemów informatycznych eksploatowanych w Szpitalu harmonogramy i miejsca tworzenia kopii zapasowych są ustalane w kartach urządzeń. Okresy i sposoby sporządzania kopii zapasowych określa Administrator Bezpieczeństwa Teleinformatycznego, a zatwierdza Pełnomocnik ds. Bezpieczeństwa. Szczegółowe zasady tworzenia kopii opisane są w Procedurze PR-05 QBP-03/E Uruchamianie systemu i odtwarzanie danych. Za wykonywanie kopii zapasowych oprogramowania i danych odpowiadają administratorzy urządzenia wymienieni w karcie urządzenia. Zasady wykonywania, wykorzystywania oraz niszczenia kopii nośników elektronicznych zostały opisane w Procedurze PR-05 QBP-03/E Uruchamianie systemu i odtwarzanie danych.

7.8 Poczta elektroniczna

Odczyt poczty elektronicznej z komputerów innych niż komputery w Szpitalu jest dozwolony tylko w bezpiecznych środowiskach – za bezpieczne środowisko uważa się służbowy komputer przenośny lub służbowy telefon komórkowy. Za środowisko bezpieczne nie uznaje się komputerów w innych podmiotach leczniczych lub publicznie dostępnych obiektach (hotele, kawiarenki internetowe, biblioteki) lub komputerów prywatnych.

W szczególności użytkownicy systemu poczty elektronicznej zobowiązani są do przestrzegania następujących zasad określonych w Regulaminie użytkownika systemu informatycznego - Załącznik nr 7 do niniejszego dokumentu oraz Procedurze PR-05 QBP-02/E Nadzór nad sprzętem komputerowym i oprogramowaniem.

Pracownicy zobowiązani są do zachowania szczególnej ostrożności przy przesyłaniu poczty elektronicznej, aby zapobiec wysłaniu wiadomości do niewłaściwego adresata.

Szpital ustanowił podstawowe zasady dotyczące wielkości wiadomości pocztowych przesyłanych (wysyłanych i odbieranych) drogą elektroniczną. Maksymalna wielkość informacji wysyłanej wynosi 5 MB, a informacji otrzymywanej wynosi 5 MB. W przypadku konieczności wysłania przesyłki o większej pojemności należy skontaktować się z Działem Informatyki.

7.9 Zasady korzystania z sieci WWW i innych usług dostępnych w Internecie

Szczegółowe zasady korzystania z internetu określono w pkt. 7.1 oraz Regulaminie użytkownika systemu informatycznego Załącznik nr 7 do niniejszego dokumentu.

W przypadku pracy na komputerze przenośnym poza terenem Szpitala zalecane jest ograniczenie korzystania z zasobów sieci WWW, aby zminimalizować ryzyko infekcji komputera przez szkodliwe oprogramowanie.

Zakazane jest wykorzystanie służbowych komputerów przenośnych do łączenia się z zasobami Szpitala w miejscach takich jak kawiarenki internetowe lub za pośrednictwem nieznanych sieci bezprzewodowych Wi-Fi oraz hot-spotów przy wykorzystaniu transmisji nieszyfrowanej.

Informuje się, że wykorzystywanie sieci WWW przez pracowników Szpitala w obrębie jego systemu informatycznego podlegają monitorowaniu.

7.10 Szyfrowanie danych

Główne zasady dotyczące zapewnienia bezpieczeństwa zawiązanego z używaniem technik kryptograficznych przy przetwarzaniu i przesyłaniu informacji Szpitala:

1. Informacje sklasyfikowane jako „poufne", które są przesyłane poza Szpital (z wyłączeniem połączeń typu VPN) podlegają szyfrowaniu według zasad określonych w Załączniku nr 4 do Procedury PR-05 QBP-02/E Nadzór nad sprzętem komputerowym i oprogramowaniem.
2. Nie jest dopuszczalne używanie własnych, nieautoryzowanych przez Pełnomocnika ds. Bezpieczeństwa, rozwiązań kryptograficznych do szyfrowania informacji klasyfikowanych jako „poufne".
3. Każdy posiadacz klucza prywatnego jest zobowiązany do jego ochrony.
4. Podejrzenie kradzieży klucza prywatnego należy bezzwłocznie zgłosić Administratorowi Bezpieczeństwa Teleinformatycznego, który jest zobowiązany do unieważnienia takiego klucza i stosownych certyfikatów oraz powiadomienia urzędu zarządzającego certyfikatami.

Szczegółowe zasady zapewnienia bezpieczeństwa zawiązanego z używaniem technik kryptograficznych przy przetwarzaniu i przesyłaniu informacji Szpitala zostały opisane w Procedurze PR-05 QBP-02/E Nadzór nad sprzętem komputerowym i oprogramowaniem.

7.11 Ochrona nośników danych

Poniższe zasady dotyczące zapewnienia bezpieczeństwa związanego z wymiennymi nośnikami informacji w Szpitalu określają zasady pracy, przechowywania i niszczenia nośników wymiennych takich jak: płyty CD/DVD, pamięci flash, pendrive, dyski optyczne, dyski USB, taśmy, inne rodzaje kart pamięci.

1. Wymienne nośniki informacji podlegają ochronie w stopniu zależnym od wymagania ochrony informacji na nich przechowywanych. W zakresie ochrony danych osobowych zabrania się przetwarzania (gromadzenia) danych osobowych na innych zasobach niż zasoby sieciowe.
2. Zabrania się korzystania z wymiennych nośników informacji (elektronicznych), na których będą przetwarzane dane osobowe lub informacje poufne bez zgody Administratora Bezpieczeństwa

Teleinformatycznego, czego potwierdzeniem powinien być wpis w rejestrze wymiennych nośników informacji.

3. Zużyte (niewykorzystywane) wymienne nośniki informacji muszą zostać sformatowane lub zniszczone mechanicznie tak, aby nie było możliwości odczytania z nich danych. W przypadku podjęcia decyzji o zniszczeniu nośnika informacji (z wyłączeniem nośników papierowych, CD, kliszy) należy przekazać go celem zniszczenia do Administratora Bezpieczeństwa Teleinformatycznego lub innego pracownika Działu Informatyki.
4. Za prawidłowe i trwałe zniszczenie nośników (z wyłączeniem papierowych) przenośnych (wyjmowanych) oraz nośników trwałych wycofanych z użycia odpowiedzialny jest Administrator Bezpieczeństwa Teleinformatycznego.
5. Wszystkie nośniki (papierowe, magnetyczne, elektroniczne, optyczne) przeznaczone do zniszczenia/odsprzedaży muszą zostać zniszczone/zabezpieczone w taki sposób, aby nie było możliwe odczytanie informacji na nich wcześniej przechowywanych. Nośniki należy niszczyć w dedykowanych do tego celu niszczarkach.
6. Do zniszczenia nośników papierowych, miękkich nośników magnetycznych oraz płyt CD/DVD zawierających dane osobowe lub inne dokumenty o charakterze poufnym za wystarczające przyjmuje się zniszczenie w niszczarkach mechanicznych o klasie niszczenia minimum DIN 2. Takiej samej metodzie niszczenia podlegają taśmy wykorzystywane do wykonywania kopii zapasowych.

7.12 Przekazywanie urządzeń do naprawy

Zasady dotyczące zapewnienia prawidłowych procedur związanych z eksploatacją i naprawą sprzętu informatycznego w Szpitalu określone są w Procedurach PR-05 QBP-01 Zgłaszania awarii oraz PR-05 QBP-02/E Nadzór nad sprzętem komputerowym i oprogramowaniem.

Użytkownik stacji roboczej powinien zgłosić jej awarię, awarię innych urządzeń peryferyjnych, błędy aplikacji, administratorowi systemu, w terminie jak najkrótszym od jej powstania zgodnie w wymaganiami procedury PR-05 QBP-01 Zgłaszanie awarii.

7.13 Wycofywanie, przekazywanie, przywracanie lub zbycie urządzeń

Zasady dotyczące zapewnieniu bezpieczeństwa w Szpitalu związane z wycofywaniem z użycia urządzeń, przekazywania ich do ponownego wykorzystania lub zbycia określone zostały w procedurach systemowych oraz Zarządzeniu Dyrektora nr 73/2012 w sprawie zasad gospodarowania mieniem ruchomym i nieruchomym WSS im. M. Kopernika w Łodzi.

7.14 Monitorowanie systemów informatycznych

Monitorowania bezpieczeństwa zasobów teleinformatycznych Szpitala określone zostały w Procedurze PR-05 QBP-02/E Nadzór nad sprzętem komputerowym i oprogramowaniem.

7.15 Prawa autorskie – licencje

Zakazane jest instalowanie na urządzeniach będących własnością (lub w użyczeniu) Szpitala oprogramowania wymagającego do instalacji/użytkowania posiadania praw licencyjnych bez zgody Administratora Bezpieczeństwa Teleinformatycznego.

Zakazane jest przechowywanie na komputerach stacjonarnych i przenośnych będących własnością Szpitala (w dzierżawie lub użyczeniu) i przekazywanie przy ich użyciu innych dokumentów elektronicznych naruszających prawo autorskie (np. filmów, nagrań i oprogramowania).

Zakazane jest wykorzystywanie systemów informatycznych Szpitala do celów niezgodnych z prawem (np. rozsyłanie niezamawianej informacji handlowej tzw. spamu, przechowywanie i dystrybuowanie nielegalnych treści, włamania na inne komputery).

8. Instrukcja postępowania w sytuacji naruszenia ochrony danych osobowych

Instrukcja określa sposób postępowania w przypadku:

- ✓ stwierdzenia naruszenia zabezpieczenia danych w systemie informatycznym,
- ✓ zaistnienia prawdopodobieństwa naruszenia zabezpieczeń danych osobowych w systemie informatycznym, na co może wskazywać: stan urządzenia, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci telekomunikacyjnej,
- ✓ stwierdzenia naruszenia zabezpieczenia danych przetwarzanych poza systemem informatycznym.

Instrukcja ma zastosowanie w szczególności wówczas, gdy stwierdzono:

- ✓ zakłócenia toku pracy ustalonych procedur działania przy przetwarzaniu danych osobowych,
- ✓ stan urządzeń wchodzących w skład systemu wskazuje na zakłócenie jego pracy,
- ✓ stan przeglądu danych osobowych lub urządzeń wchodzących w skład systemu informatycznego wskazuje na obecność wirusa zakłócającego normalny tok pracy,
- ✓ włamanie lub innego rodzaju naruszenie zabezpieczeń stosowanych w obszarze przetwarzania danych osobowych,

- ✓ ujawnienia osobom nieuprawnionym danych osobowych ze zbioru danych objętych systemem zabezpieczeń,
- ✓ rażącego naruszenie zasad i dyscypliny pracy w zakresie bezpieczeństwa danych osobowych chronionych przepisami ustawy o ochronie danych osobowych,
- ✓ zniszczenia, uszkodzenie lub zniknięcie zbioru danych osobowych lub jego poszczególnych części.

W przypadku stwierdzenia przez osobę przetwarzającą dane osobowe lub jej przełożonego, zaistnienia choćby jednej z przesłanek, o których mowa powyżej, osoby te są zobowiązane natychmiast zawiadomić o tym Administratora Bezpieczeństwa Fizycznego i Osobowego.

Administrator Bezpieczeństwa Fizycznego i Osobowego lub osoba imiennie przez niego wskazana w obecności pracownika, który stwierdził naruszenie zabezpieczeń lub zasad ochrony danych osobowych – przeprowadza oględziny miejsca stwierdzenia naruszenia i sporządza na tę okoliczność raport wystąpienia zdarzenia lub incydentu bezpieczeństwa.

Raport powinien zawierać w szczególności:

- ✓ datę, godzinę i miejsce jego sporządzenia,
- ✓ określenie osób obecnych przy jego sporządzaniu,
- ✓ precyzyjne wskazanie stwierdzonego naruszenia zasad związanych z ochroną przetwarzania danych osobowych lub zabezpieczeń stosowanych w tym zakresie w systemie informatycznym, gdzie przetwarzane są dane lub poza systemem informatycznym,
- ✓ wskazanie terminu stwierdzenia naruszenia ochrony danych,
- ✓ określenie szkód i zagrożenia dla danych przetwarzanych w zbiorze,
- ✓ wskazanie osób odpowiedzialnych za naruszenie zabezpieczeń,
- ✓ podpisy osób obecnych przy oględzinach.

Po sporządzeniu protokołu Komitet ds. Bezpieczeństwa dokonuje analizy i oceny całokształtu stwierdzonego naruszenia zasad ochrony danych osobowych, następnie zarządza wprowadzenie środków eliminujących w przyszłości podobne zdarzenia, przeprowadza modernizację i bieżący monitoring zabezpieczeń danych osobowych zarówno w systemie informatycznym jak i poza tym systemem.

W przypadku stwierdzenia ewidentnego naruszenia dyscypliny pracy przez osobę zatrudnioną przy przetwarzaniu danych osobowych, ABFiO niezwłocznie powiadamia o tym fakcie Administratora Danych Osobowych - Dyrektora Szpitala celem przedsięwzięcia środków dyscyplinujących.

9. Zarządzanie ciągłością działania

W celu zapewnienia ciągłości działania Szpitala i możliwości odtworzenia kluczowych elementów procesów biznesowych opracowany został Plan postępowania na wypadek sytuacji nadzwyczajnej na terenie Szpitala. W zależności od rodzaju zdarzenia plan zawiera szczegółowe algorytmy postępowania - *Plany Ciągłości Działania*. Celem takiego planu jest ograniczanie zagrożeń organizacyjnych do poziomu uznanego przez kierownictwo Szpitala za dopuszczalne. Przy opracowywaniu Planów Ciągłości Działania uwzględniono wymagania wynikające z powszechnie obowiązujących przepisów prawa, a także polskich i międzynarodowych norm oraz zwyczajów.

Plany Ciągłości Działania są okresowo przeglądane przez Komitet ds. Bezpieczeństwa pod kątem aktualności i przydatności. Przeglądy planów są przeprowadzane z częstotliwością nie rzadziej niż raz na dwa lata lub w razie potrzeby częściej - po każdej znaczącej zmianie w Szpitalu dotyczącej systemów, oprogramowania, struktury organizacyjnej, struktury zatrudnienia czy wyposażenia budynku.

10. Załączniki

Załącznik nr 1 – anulowano Kartą zmian nr 14/2013

Załącznik nr 2 - anulowano Kartą zmian nr 14/2013

Załącznik nr 3 – Wykaz osób pełniących funkcje w ramach SZBI,

Załącznik nr 4 – Klasyfikacja informacji,

Załącznik nr 5 - Komitet ds. Bezpieczeństwa,

Załącznik nr 6 – Deklaracja stosowania,

Załącznik nr 7 – Regulamin użytkownika systemu informatycznego.