**Polityka Bezpieczeństwa Informacji Samodzielnym Publicznym Zakładzie Opieki Zdrowotnej w Myślenicach**

1. Zapewniając bezpieczeństwo informacji zidentyfikowane zostały procesy jakie są realizowane w Podmiocie leczniczym Samodzielny Publiczny Zakład Opieki Zdrowotnej w Myślenicach oraz aktywa informacyjne, które wymagają ochrony. W celu skutecznej ochrony informacji powierzonych przez pacjentów, kontrahentów, pracowników i wszelkich innych podmiotów oraz powstających w procesie realizacji usług wdrożyliśmy i stosujemy System Zarządzania Bezpieczeństwem Informacji.
2. System zarządzania bezpieczeństwem informacji jaki jest wdrożony w Samodzielnym Publicznym Zakładzie Opieki Zdrowotnej w Myślenicachbazuje na identyfikacji i klasyfikacji informacji, które chcemy chronić. Jesteśmy świadomi, że informacje, niezależnie od nośnika, na którym są gromadzone oraz kanałów informacyjnych, którymi są przekazywane powinny być chronione w taki sposób, aby nie następowało ich nieautoryzowane ujawnienie, przekazanie lub wykorzystanie, które mogłoby prowadzić do naruszenia interesów i praw naszych interesariuszy. Niezmiernie istotne jest, aby wszystkie informacje były właściwie chronione, a także dostępne na czas dla osób upoważnionych oraz aby nie ulegały nieautoryzowanym zniekształceniom na skutek umyślnego lub nieumyślnego działania.
3. Aby spełnić wymagania w zakresie bezpieczeństwa informacji wszyscy pracownicy powinni stosować się do wymagań wynikających z niniejszej polityki, deklaracji stosowania zabezpieczeń oraz dokumentacji systemu zarządzania bezpieczeństwem informacji.
4. Dla zapewnienia wysokiego poziomu bezpieczeństwa informacji stosujemy następujące zasady:
5. aktywa informacyjne są poddawane regularnym przeglądom,
6. regularnie wykonywany jest proces oceny ryzyka w celu coraz lepszej identyfikacji zagrożeń związanych z wykorzystywanymi aktywami,
7. stale podnosimy świadomość pracowników w zakresie bezpieczeństwa informacji,
8. kładziemy duży nacisk na stosowanie nowoczesnych i bezpiecznych technologii informacyjnych,
9. zwracamy szczególną uwagę na dobór dostawców oraz odpowiedni nadzór nad powierzonymi im procesami i informacjami,
10. zbieramy i analizujemy wszelkie incydenty związane z naruszeniem bezpieczeństwa informacji oraz podejmujemy niezwłoczne działania w celu wyeliminowania tych zagrożeń w przyszłości,
11. identyfikujemy zobowiązania prawne oraz kontraktowe, a także oczekiwania petentów,
12. stale monitorujemy skuteczność stosowanych zabezpieczeń,
13. kładziemy duży nacisk na ciągłe doskonalenie systemu zarządzania bezpieczeństwem informacji,
14. Wszyscy pracownicy zobowiązani są do przestrzegania wymagań bezpieczeństwa informacji określonych w dokumentacji oraz tych wynikających z wymagań prawnych i innych.
15. Pracownicy Podmiotu leczniczego zobowiązani są do:
16. dbałości o bezpieczeństwo powierzonych informacji,
17. stosowania zabezpieczeń w odniesieniu do informacji i sprzętu służącego do tworzenia, przechowywania i przetwarzania informacji,
18. ochrony danych osobowych,
19. zgłaszania wszystkich stwierdzonych przypadków naruszenia bezpieczeństwa informacji,
20. zgłaszania propozycji rozwiązań systemowych i organizacyjnych służących poprawie poziomu bezpieczeństwa informacji.

(miejscowość), dnia ……………….…….…*……………………………………….……*

 *Podpis Dyrektora*