I. ZASADY OGÓLNE.

1. Celem polityki jest zapewnienie ochrony aktywów informacyjnych udostępnianych usługodawcom, dostawcom i innym osobom oraz podmiotom zewnętrznym wykonującym czynności w imieniu i na rzecz „CENTRUM MEDYCZNEGO” Sp. z o. o w Rybniku.
2. Przedmiotowe zasady i wymogi dot. w szczególności:
   a) udostępniania aktywów informacyjnych oraz monitorowania i kontroli dostępu,
   b) przestrzegania określonych zasad i wymogów przez podmioty zewnętrzne,
   c) przestrzegania obowiązków podmiotów zewnętrznych w zakresie zapewnienia ochrony aktywów informacyjnych,
   d) zgłaszania przypadków naruszenia lub podejrzenia naruszenia bezpieczeństwa informacji,
   e) uświadamiania pracowników podmiotów zewnętrznych w zakresie bezpieczeństwa informacji,
   f) postępowania z poufnymi informacjami, w tym powierzonymi podmiotom zewnętrznym danymi osobowymi.
3. Zapisy niniejszego dokumentu mają charakter uzupełniający do treści PBTI.
4. Niniejsza Polityka bezpieczeństwa podlega przeglądom pod kątem aktualności, przydatności i adekwatności.
5. Wykonawca będący stroną zawartej umowy lub porozumienia zobowiązany jest do zapoznania podległych mu pracowników realizujących przedmiot ww. umowy lub porozumienia z zasadami ochrony aktywów informacyjnych CM w szczególności w PBTI.
6. Pracownicy współpracujących podmiotów zewnętrznych zobowiązani są do przestrzegania zasad ochrony aktywów informacyjnych określonych w Politykach.

II. PRZYZNAWANIE DOSTĘPU PODMIOTOM ZEWNĘTRZNYM DO AKTYWÓW INFORMACYJNYCH „CENTRUM MEDYCZNEGO” Sp. z o.o.

1. Pracownicy podmiotów zewnętrznych, realizujący określone zadania na podstawie zawartej umowy cywilnoprawnej lub porozumienia mogą otrzymać dostęp do aktywów informacyjnych CM oraz aktywów wspierających przetwarzanie informacji: sprzęt (w tym komputery, nośniki informacji, oprogramowanie).
2. Przyznawanie, zmiana, ograniczenie i odbieranie praw dostępu do aktywów informacyjnych podmiotom zewnętrznym odbywa się zgodnie z PBTI i obowiązującymi przepisami prawa, na formalny wniosek o nadanie praw dostępu.
3. Pracownicy podmiotów zewnętrznych mają swobodny dostęp do ogólnodostępnej strefy bezpieczeństwa obejmującej wejścia do budynków, korytarze oraz wybrane pomieszczenia nie stanowiące pomieszczeń ograniczonego dostępu.
4. Pracownicy podmiotów zewnętrznych mogą uzyskać dostęp do strefy chronionej lub specjalnej po uzyskaniu zgody Prezesa/Prokurenta.
5. W strefie specjalnej (serverownia, kasa) pracownicy podmiotów zewnętrznych mogą przebywać tylko pod ścisłym nadzorem ASI lub upoważnionym pracownikiem administracji.

6. W przypadku konieczności nadania uprawnień do systemu informatycznego dla stron trzecich takich jak np. serwisanci oprogramowania, przydzielane jest konto z nazwą identyfikującą daną firmę wraz z odpowiednim poziomem uprawnień (zał. Nr 1A PBTI) oraz oświadczenie zgodne ze wzorem określonym w załączniku nr 7 i 7A PBTI. Jeżeli zachodzi konieczność prac na koncie administratora to odbywają się one tylko pod kontrolą ASI. Po każdorazowej pracy serwisantów hasło do konta zostaje zmienione.

III. PODSTAWOWE ZASADY BEZPIECZEŃSTWA W ZAKRESIE WSPÓŁPRACY Z PODMIOTAMI ZEWNĘTRZNYMI

1. W uzupełnieniu do zasad i wymogów określonych w PBTI podmioty zewnętrzne w ramach współpracy z CM zobowiązane są przestrzegać niniejszych zasad bezpieczeństwa dot. przedmiotowej współpracy.
2. W przypadku korzystania z budynków i pomieszczeń CM, pracownicy podmiotów zewnętrznych zobowiązani są również do zapoznania i stosowania się do zapisów obowiązującej instrukcji przeciwpożarowej i przepisów BHP.
3. Ww. podmioty zobowiązane są do przestrzegania „zasady czystego biurka i ekranu” oraz dbać o bezpieczeństwo powierzonych im aktywów, a w szczególności chronić przed utratą, kradzieżą, nieuprawnioną modyfikacją, uszkodzeniami mechanicznymi.
4. Pracownikom podmiotów zewnętrznych nie wolno podejmować prób sprawdzania, testowania i omijania zabezpieczeń powierzonych im aktywów informacyjnych, w tym:
   a) samowolnie modyfikować ustawień związanych z bezpieczeństwem,
   b) świadomie wprowadzać błędnych danych,
   c) podejmować prób przywłaszczenia lub rozszyfrowania informacji uwierzytelniających innych użytkowników.
5. W ramach zapewnienia poufności informacji przetwarzanych w CM, pracownicy podmiotów zewnętrznych zobowiązani są zachować w tajemnicy przez czas nieokreślony (w trakcie jak i po zakończeniu trwania umowy) informacje udostępnione im w związku z realizacją umowy oraz chronić je przed ujawnieniem osobom nieuprawnionym.
6. Wymóg zachowania poufności, o którym mowa w pkt. 5 obejmuje wszelkie informacje, których ujawnienie mogłoby narazić „CENTRUM MEDYCZNE” na szkodę. Przedmiotowy wymóg nie dotyczy informacji, które są jawne i/lub ogólnodostępne.

IV. ZGŁASZANIE PRZYPADKÓW NARUSZENIA BEZPIECZEŃSTWA INFORMACJI PRZEZ PODMIOTY ZEWNĘTRZNE

1. Pracownicy podmiotów zewnętrznych, zleceniobiorcy oraz inne osoby i podmioty zewnętrzne wykonujące czynności w imieniu i na rzecz „CENTRUM MEDYCZNEGO” Sp. z o.o. i/lub mające dostęp do aktywów informacyjnych w przypadku zaistnienia okoliczności mogących świadczyć o naruszeniu bezpieczeństwa informacji w „CENTRUM MEDYCZNYM” zobowiązani są

niezwłocznie poinformować o szczegółach i charakterze zdarzenia Prezesa „CENTRUM MEDYCZNEGO” Sp. z o.o.

2. Próby/przypadki nieautoryzowanego dostępu do aktywów informacyjnych są identyfikowane jako incydenty związane z bezpieczeństwem informacji.
3. Naruszenie postanowień umowy lub wymogów obowiązującej dokumentacji bezpieczeństwa przez podmiot zewnętrzny stanowi podstawę do odstąpienia od umowy i żądania pokrycia powstałej szkody lub zapłaty kary umownej, jeżeli taki obowiązek wynikał z zawartej umowy.
4. Z tytułu działań podmiotów zewnętrznych i jego przedstawicieli, niezgodnych z przepisami prawa powszechnie obowiązującego (w tym dot. przetwarzania danych osobowych), grożą odrębne kary określone w szczególności w kodeksie pracy, kodeksie cywilnym, kodeksie karnym, przepisów RODO oraz ustawie o ochronie danych osobowych.

V. ZASADY WSPÓŁPRACY Z PODMIOTAMI ZEWNĘTRZNYMI W PRZYPADKU NARUSZENIA BEZPIECZEŃSTWA INFORMACJI

1. Zgodnie z RODO, przypadki naruszenia ochrony danych osobowych prowadzącego do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych zostaną niezwłocznie zgłoszone organowi nadzorczemu.

Kopia:	Własność:

	Stanowisko	**Data**	**Nazwisko i imię**	**Podpis**
Opracował:	Zespół Sterujący	10.01.2020r.	mgr Aleksander Brzęska lek.med. Janusz Ostrowski, Teresa Kopeć	
Zatwierdził:	Prezes - ADO	15.01.2020r.	mgr Aleksander Brzęska