Załącznik nr 1
do Zarządzenia nr ……/2022 Dyrektora - Członka Zarządu
Europejskiego Centrum Zdrowia Otwock sp. z o.o.

Polityka ciągłości działania

OPRACOWAŁ	WŁAŚCICIEL PROCEDURY
ODO Consulting sp. z o.o.	Pełnomocnik ds. SZBI
Data i podpis:	Data i podpis:
SPRAWDZIŁ	**ZATWIERDZIŁ**
Dyrektor Techniczny	Dyrektor - Członek Zarządu
Data i podpis:	Data i podpis:

Celem wprowadzenia w Szpitalu Systemu Zarządzania Ciągłością Działania, jest zapewnienie o nieprzerwalności w realizacji zadań statutowych w sposób uporządkowany - w tym usług kluczowych – na wypadek wystąpienia nagłych zdarzeń lub nieszczęśliwych wypadków.

System Zarządzania Ciągłością Działania, ma na celu minimalizację zakłóceń w realizacji działalności statutowej oraz określenie planu postępowania w przypadku zaistnienia zdarzeń mających wpływ (również potencjalny) na bezpieczeństwo informacji oraz ciągłości działania Szpitala.

Na System Zarządzania ciągłością działania, składają się:

a) Polityka Ciągłości Działania;
b) Plan Ciągłości Działania.

Użyte w niniejszej Polityce pojęcia mają następujące znaczenie:

Pojęcie	Definicja
Bezpieczeństwo informacji	zachowanie poufności, integralności i dostępności informacji; dodatkowo, mogą być brane pod uwagę inne własności, takie jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność;
Centralny Zespół ds. Reagowania na Incydenty (CZRI)	wewnętrzna struktura odpowiedzialna za cyberbezpieczeństwo w Szpitalu powołana odrębnym Zarządzeniem Dyrektora - Członka Zarządu Szpitala;
Ciągłość działania	zdolność Szpitala do ciągłego świadczenia usług w akceptowalnych ramach czasowych przy zdefiniowanej wcześniej zdolności do działania w czasie zakłócenia;
Naruszenie bezpieczeństwa informacji	przypadek, w którym użytkownik lub inna osoba pomija lub niszczy ustanowione zabezpieczenia lub środki ochrony w celu pozyskania nieuprawnionego dostępu do informacji lub do pozostałych zasobów systemu informatycznego;
Plan ciągłości działania	udokumentowany zbiór procedur awaryjnych i informacji, które są opracowane, gromadzone i utrzymywane w stanie gotowym do użycia w przypadku wystąpienia incydentu, aby umożliwić Szpitalowi kontynuowanie wykonywanych działań krytycznych na możliwym do przyjęcia wcześniej określonym poziomie;
Plan odtworzeniowy	dokument zawierający szczegółowy opis postępowania w przypadku wystąpienia określonego zdarzenia (awarii lub katastrofy), mającego na celu usunięcie skutków lub przyczyn awarii lub katastrofy;
Szpital	Europejskie Centrum Zdrowia Otwock sp. z o.o.;
UKSC	ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa;

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 powoduje, że ryzyko materializuje się w postaci wymiernej straty poprzez wystawienie danych osobowych na utratę, ujawnienie, zniszczenie lub zmianę;
Zagrożenie cyberbezpieczeństwa	potencjalna przyczyna wystąpienia incydentu;
Zarządzanie incydentem	obsługa incydentu, wyszukiwanie powiązań między incydentami, usuwanie przyczyn ich wystąpienia oraz opracowywanie wniosków wynikających z obsługi incydentu;
Zarządzanie ryzykiem	skoordynowane działania w zakresie zarządzania cyberbezpieczeństwem w odniesieniu do oszacowanego ryzyka; systematyczne stosowanie zasad zarządzania, procedur i praktyk na rzecz działań w zakresie informowania, konsultowania, tworzenia kontekstu oraz identyfikowania, analizy, oceny, postępowania z ryzykiem, monitorowania i przeglądania ryzyka związanego z przetwarzaniem informacji;
Zarządzanie ciągłością działania	całościowy proces zarządzania identyfikujący potencjalne zagrożenia i skutki, jakie te zagrożenia mogą wywierać na działalność Szpitala w przypadku ich wystąpienia, który zapewnia kształtowanie odporności Szpitala i umożliwia skuteczną reakcję w celu ochrony interesów kluczowych interesariuszy tj. osób zaangażowanych w działalność Szpitala, reputacji i wizerunku Szpitala;
Zdarzenie związane z bezpieczeństwem informacji	stwierdzone wystąpienie stanu systemu, usługi lub sieci, który wskazuje na możliwe naruszenie polityki bezpieczeństwa informacji lub błąd zabezpieczenia, lub nieznaną dotychczas sytuację, która może być związana z bezpieczeństwem informacji;
Zespół ds. Zarządzania Ciągłością Działania	wewnętrzna struktura odpowiedzialna za zarządzanie ciągłością działania w Szpitalu powołana odrębnym Zarządzeniem Dyrektora - Członka Zarządu Szpitala.

1. Szpital jest jednostką, która ma za zadanie w szczególności realizować zadania ustawowe i w związku z realizacją tych zadań jest zobowiązany do zapewnienia poufności, integralności oraz dostępności danych w tym danych osobowych, które przetwarza w wyżej wymienionych celach. Wszystkie czynności przetwarzania, które Szpital wykonuje, są realizowane w oparciu o wartości będące fundamentem misji oraz celów Szpitala. Zapewnienie ciągłości działania usługi kluczowej polegającej na „udzielaniu świadczeń opieki zdrowotnej przez podmiot leczniczy oraz obrocie i dystrybucji produktów leczniczych" jest wpisane również w strategię Szpitala.

2. Główne cele ciągłości działania obejmują:

   1) zapobieganie niezaplanowanym przerwom w realizacja procesów i zadań Szpitala,
   2) utrzymywanie właściwej i niezawodnej infrastruktury technicznej niezbędnej do ich realizacji,
   3) monitorowanie i ograniczanie potencjalnych zagrożeń w środowisku pracy, w tym identyfikację i ocenę zdarzeń niepewnych, które mogą mieć wpływ na realizowane przez Szpital zadania,
   4) stałe podnoszenie świadomości pracowników w zakresie utrzymania ciągłości działania i ich roli w przypadku wystąpienia sytuacji kryzysowej.

3. Szpital uwzględniając wymogi prawne zobowiązuje się do:
   a) przygotowania, utrzymywania, przeglądania i doskonalenia procedur SZCD,
   b) odtworzenia kluczowych usług w przypadku wystąpienia zakłócenia,
   c) zapewnienia niezbędnych zasobów do utrzymania SZCD,
   d) wdrożenia działań zmniejszających ryzyko wystąpienia zakłóceń,
   e) sprawnego komunikowania niniejszej Polityki Ciągłości Działania oraz aktualnych Planów Ciągłości Działania,
   f) utrzymania współpracy z dostawcami usług w tym ekspertami technicznymi, którzy są niezbędni dla zapewnienia realizacji Planów Ciągłości Działania.

4. Polityką Ciągłości Działania związany jest cały Personel Szpitala, a także wyznaczeni przez Szpital dostawcy usług w tym eksperci techniczni.

5. Zespół ds. Zarządzania Ciągłością Działania odpowiada za koordynowanie działań organizacji zarówno w trakcie wystąpienia zakłócenia, jak i w warunkach bieżącej działalności organizacji. Zespół odpowiada także za aktualność wszystkich ustanowionych Planów Ciągłości Działania w tym uczestniczy w przeglądzie zarządzania SZCD.

6. Dział Informatyczny odpowiada za:
   1) identyfikowanie zagrożeń w odniesieniu do systemów informacyjnych Szpitala oraz proponowanie rozwiązań ograniczających ryzyko wynikające z tych zagrożeń,

2) analizowanie oprogramowania szkodliwego i określanie jego wpływu na system informacyjny Szpitala;
3) wykrywanie przełamania lub ominięcia zabezpieczeń systemu informacyjnego Szpitala, prowadzenie analizy powłamaniowej wraz z określeniem działań niezbędnych do przywrócenia sprawności systemu informacyjnego Szpitala,
4) zabezpieczanie informacji potrzebnych do analizy powłamaniowej, pozwalających na określenie wpływu incydentu poważnego na świadczenie usługi kluczowej, w tym informacji dotyczących:
    a) rodzajów usług kluczowych, na które incydent miał wpływ,
    b) liczby użytkowników usługi kluczowej, na których incydent miał wpływ,
    c) momentu wystąpienia i wykrycia incydentu oraz czas jego trwania,
    d) zasięgu geograficznego obszaru, którego dotyczy incydent poważny,
    e) wpływu incydentu na świadczenie usługi kluczowej przez innych operatorów usług kluczowych i dostawców usług cyfrowych,
    f) przyczyny zaistnienia incydentu i sposobu jego przebiegu oraz skutków jego oddziaływania na systemy informacyjne lub świadczone usługi kluczowe na potrzeby postępowań prowadzonych przez organy ścigania.

7. Najwyższe kierownictwo sprawuje nadzór w zakresie funkcjonowania SZCD.

8. Ćwiczenia i testy w omawianym obszarze, przeprowadzane są zgodnie z ustalonym przez Szpital harmonogramem.

9. Personel Szpitala jest na bieżąco szkolony, w ustalonych odstępach czasu, tak by w sytuacji wystąpienia zakłócenia każdy z Personelu Szpitala, wiedział jaka jest jego rola i odpowiedzialność w SZCD.

10. Polityka Ciągłości Działania jest dostępna dla stron zainteresowanych w udokumentowanej formie, a także jest komunikowana na wszystkich szczeblach struktury Szpitala.

Dokumenty powiązane I poziomu SZBI:

1. BI-1-P – Polityka Bezpieczeństwa Informacji;

Dokumenty powiązane II poziomu SZBI:

2. BI-2-U – Polityka ochrony danych osobowych;
3. BI-3-U – Polityka zarządzania ryzykiem;
4. BI-4-U – Polityka zarządzania incydentem;
5. BI-5-U – Polityka użytkowania sieci teleinformatycznej;
6. BI-7-U – Polityka zarządzania aktywami informacyjnymi;
7. BI-8-U – Polityka bezpieczeństwa fizycznego i środowiskowego;
8. BI-10-U – Polityka monitorowania i nadzoru nad bezpieczeństwem informacji.

Dokumenty powiązane III poziomu SZBI:

9. BI-6-1-U – Plan ciągłości działania.

Dokumenty związane:

1. Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa;
2. Rozporządzenie Rady Ministrów z dnia 31 października 2018 r. w sprawie progów uznania incydentu za poważny;
3. Rozporządzenie Rady Ministrów z dnia 11 września 2018 r. w sprawie wykazu usług kluczowych oraz progów istotności skutku zakłócającego incydentu dla świadczenia usług kluczowych;
4. Rozporządzenie Ministra Cyfryzacji z dnia 4 grudnia 2019 r. w sprawie warunków organizacyjnych i technicznych dla podmiotów świadczących usługi z zakresu cyberbezpieczeństwa oraz wewnętrznych struktur organizacyjnych operatorów usług kluczowych odpowiedzialnych za cyberbezpieczeństwo;
5. Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych;
6. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych

osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).

Podpisy złożono na oryginale dokumentu.