DOKUMENTACJA
ZINTEGROWANEGO SYSTEMU ZARZĄDZANIA

TYTUŁ: PP/03 - SZBI Polityka ciągłości działania

WŁAŚCICIEL PROCEDURY: Pełnomocnik ds. Jakości

Opracował	Sprawdził	Zatwierdził
ODO Consulting sp. z o.o., Warszawa	Barbara Tyfa – Pełnomocnik Dyrektora ds. Jakości, Bartłomiej Pałka – Kierownik Sekcji Informatyki	Dr hab. n.med. Iwona Maroszyńska prof. ICZMP – Dyrektor
Data: 13. 09. 2023 r.	Data: 13. 09. 2023 r.	Data:

I. CEL PROCEDURY

Celem wprowadzenia w ICZMP 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 ICZMP.

II. PRZEDMIOT I ZAKRES PRCPOEDURY

Na System Zarządzania ciągłością działania, składają się:

a) Polityka Ciągłości Działania;
b) Plany ciągłości działania.

III. TERMINOLOGIA I DEFINICJE

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 ICZMP powołana odrębnym Zarządzeniem Dyrektora ICZMP;
Ciągłość działania	zdolność ICZMP 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 ICZMP 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;
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 ICZMP w przypadku ich wystąpienia, który zapewnia kształtowanie odporności ICZMP i umożliwia skuteczną reakcję w celu ochrony interesów kluczowych interesariuszy tj. osób zaangażowanych w działalność ICZMP, reputacji i wizerunku ICZMP;
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. Cyberbezpieczeństwa	zespół osób powołany Zarządzeniem Dyrektora ICZMP, realizujący zadania wskazane w art. 8 pkt. 4 i 6, art. 11 ust. 1 pkt. 1-5, art. 12 i art. 13 UKSC;
Zespół ds. Zarządzania Ciągłością Działania	wewnętrzna struktura odpowiedzialna za zarządzanie ciągłością działania w ICZMP powołana odrębnym Zarządzeniem Dyrektora ICZMP.

IV. ODPOWIEDZIALNOŚCI I UPRAWNIENIA

1. ICZMP 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 ICZMP wykonuje, są realizowane w oparciu o wartości będące fundamentem misji oraz celów ICZMP. 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 ICZMP.

2. Główne cele ciągłości działania obejmują:

   1) zapobieganie niezaplanowanym przerwom w realizacja procesów i zadań ICZMP,
   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 ICZMP zadania,
   4) stałe podnoszenie świadomości pracowników w zakresie utrzymania ciągłości działania i ich roli w przypadku wystąpienia sytuacji kryzysowej.

3. ICZMP jako podmiot odpowiedzialny za realizację kluczowej usługi, 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 ICZMP, a także wyznaczeni przez ICZMP 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. Zespół ds. cyberbezpieczeństwa odpowiada za:
   1) identyfikowanie zagrożeń w odniesieniu do systemów informacyjnych ICZMP oraz proponowanie rozwiązań ograniczających ryzyko wynikające z tych zagrożeń,
   2) analizowanie oprogramowania szkodliwego i określanie jego wpływu na system informacyjny ICZMP;
   3) wykrywanie przełamania lub ominięcia zabezpieczeń systemu informacyjnego ICZMP, prowadzenie analizy powłamaniowej wraz z określeniem działań niezbędnych do przywrócenia sprawności systemu informacyjnego ICZMP,
   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 ICZMP harmonogramem.

9. Personel ICZMP jest na bieżąco szkolony, w ustalonych odstępach czasu, tak by w sytuacji wystąpienia zakłócenia każdy z Personelu ICZMP, 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 ICZMP.

V. DOKUMENTY ZWIĄZANE:

1. PP/01 – SZBI - Polityka bezpieczeństwa informacji
2. PP/02 – SZBI - Polityka ochrony danych osobowych
3. PP/04 – SZBI - Procedura nadawania upoważnień;
4. PP/05 – SZBI - Procedura udostępniania danych;
5. PP/06 – SZBI - Procedura powierzenia przetwarzania danych;
6. PP/07 – SZBI - Procedura oceny skutków;
7. PP/08 – SZBI - Procedura zarządzania ryzykiem bezpieczeństwa informacji;
8. PP/09 – SZBI - Procedura zarządzania podatnościami;
9. PP/10 – SZBI - Procedura zarządzania incydentami związanymi z bezpieczeństwem informacji;
10. PP/11 – SZBI - Procedura użytkowania sieci teleinformatycznej;
11. PP/12 – SZBI - Procedura rejestracji i inwentaryzacji oprogramowania i sprzętu komputerowego;
12. PP/13 – SZBI - Procedura pracy zdalnej;
13. PP/14 – SZBI - Procedura dostępu VPN do zasobów sieci ICZMP;
14. PP/15 – SZBI - Procedura przechowywania i przekazywania hasła administratora systemu;
15. PP/16 – SZBI - Procedura wykonywania kopii zapasowych;
16. PP/17 – SZBI - Procedura rejestracji i inwentaryzacji sprzętu medycznego;
17. PP/18 – SZBI - Procedura zarządzania zmianą IT;
18. PP/19 – SZBI - Procedura privacy by design, privacy by default;
19. PP/20 – SZBI - Procedura zarządzania aktywami informacyjnymi;
20. PP/21 – SZBI - Procedura zarządzania bezpieczeństwem zasobów ludzkich;
21. PP/22 – SZBI - Procedura bezpieczeństwa fizycznego i środowiskowego;
22. PP/23 – SZBI - Procedura zarządzania kluczami;
23. PP/24 – SZBI - Procedura zarządzania uprawnieniami w systemie kontroli dostępu;
24. PP/25 – SZBI - Procedura dostępu do serwerowni;
25. PP/26 – SZBI - Procedura zarządzania systemem monitoringu wizyjnego;
26. PP/27 – SZBI - Procedura korzystania z bezprzewodowej sieci dla pracownika;
27. PP/28 – SZBI - Procedura korzystania z bezprzewodowej sieci dla gości;
28. PP/29 – SZBI - Procedura bezpieczeństwa w relacjach z podmiotami zewnętrznymi dla pracowników;
29. PP/30 – SZBI - Procedura bezpieczeństwa w relacjach z podmiotami zewnętrznymi dla dostawców;
30. PP/31 – SZBI - Procedura monitorowania i nadzoru nad bezpieczeństwem informacji.

VI. PODSTAWA PRAWNA:

1. Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa;
2. 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);
3. Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych;
4. Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne;
5. Ustawa z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta;

6. Ustawa z dnia z dnia 15 kwietnia 2011 r. o działalności leczniczej;
7. Ustawa z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia;
8. Ustawa z dnia 27 sierpnia 2004 r. o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych;
9. Ustawy z dnia z 27 sierpnia 2009 r. o finansach publicznych;
10. Ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej;
11. Ustawa z dnia 11 września 2019 r. prawo zamówień publicznych;
12. Ustawa z dnia 26 czerwca 1974 r. Kodeks pracy;
13. Ustawa z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach;
14. Ustawa z dnia 4 lutego 1994 roku o prawie autorskim i prawach pokrewnych;
15. Ustawa z dnia 29 września 1994 roku o rachunkowości;
16. Ustawa z dnia 6 czerwca 1997 r. Kodeks karny;
17. Ustawa z dnia 22 sierpnia 1997 r. o ochronie osób i mienia;
18. Ustawa z dnia 27 lipca 2001 roku o ochronie baz danych;
19. Ustawa z dnia 16 grudnia 2016 r. o zasadach zarządzania mieniem państwowym;
20. Ustawa z dnia 18 lipca 2002 roku o świadczeniu usług drogą elektroniczną;
21. Rozporządzenie Rady Ministrów z dnia 31 października 2018 r. w sprawie progów uznania incydentu za poważny;
22. Rozporządzenie Rady Ministrów z dnia 11 września 2018 r. w sprawie wykazu usług kluczowych oraz progów istotności skutku zakłócającego incydentu dla świadczenia usług kluczowych;
23. 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;
24. Rozporządzenie Rady Ministrów z dnia 16 października 2028 r. w sprawie rodzajów dokumentacji dotyczącej cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej;
25. Rozporządzenie Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu;
26. 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;
27. Rozporządzenie Ministra Zdrowia z dnia 8 maja 2018 r. w sprawie rodzajów elektronicznej dokumentacji medycznej;
28. Rozporządzenie Ministra Zdrowia z dnia 6 kwietnia 2020 r. w sprawie rodzajów, zakresu i wzorów dokumentacji medycznej oraz sposobu jej przetwarzania.

VII. ZAŁĄCZNIK: