DOKUMENTACJA
ZINTEGROWANEGO SYSTEMU ZARZĄDZANIA

TYTUŁ: PP/30 - SZBI Procedura bezpieczeństwa w relacjach z podmiotami zewnętrznymi dla dostawców

WŁAŚCICIEL PROCEDURY: Pełnomocnik ds. SZBI

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 procedury jest zapewnienie ochrony aktywów informacyjnych udostępnianych podmiotom zewnętrznym wykonującym czynności w imieniu i na rzecz Instytutu „Centrum Zdrowia Matki Polki" w Łodzi lub mającym dostęp do aktywów ICZMP oraz utrzymania ciągłości realizacji usług świadczonych przez ww. podmioty.

II. PRZEDMIOT I ZAKRES PROCEDURY

Przedmiotem procedury jest określenie zasad i wymogów bezpieczeństwa i ciągłości działania. Przedmiotowe zasady i wymogi dot. w szczególności:

1) obowiązków podmiotów zewnętrznych w zakresie zapewnienia ochrony aktywów informacyjnych ICZMP i ciągłości świadczonych usług,
2) zgłaszania przypadków naruszenia lub podejrzenia naruszenia bezpieczeństwa informacji lub ciągłości działania,
3) dodatkowych wymogów w zakresie utrzymania ciągłości realizacji procesów krytycznych.

Zapisy niniejszego dokumentu mają charakter uzupełniający do treści Polityki Bezpieczeństwa Informacji (BI-1-P) i Polityki Ciągłości Działania (BI-6-P) ICZMP oraz dokumentów II i III poziomu SZBI, tworząc wspólnie kompleksową dokumentację bezpieczeństwa i ciągłości działania.

III. TERMINOLOGIA I DEFINICJE

Pojęcie	Definicja
Administrator	osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych. W niniejszej dokumentacji ochrony danych osobowych przez administratora danych rozumie się ICZMP;
Aktywa	wszystko, co ma wartość dla ICZMP, a w szczególności: personel, wizerunek, informacje wytwarzane, przetwarzane i przechowywane w ICZMP, mienie wykorzystywane przez ICZMP oraz jej personel, i z tego powodu wymaga ochrony;
Aktywa informacyjne	kluczowe procesy i zadania, informacje przetwarzane w dowolnej formie, w tym papierowej i elektronicznej w ramach ww. procesów i zadań oraz aktywa wspierające przedmiotowe przetwarzanie, posiadające wartość dla ICZMP i wymagające właściwej ochrony przed utratą dostępności, poufności i integralności;
Centralny Zespół ds. Reagowania na Incydenty (CZRI)	wewnętrzna struktura odpowiedzialna za cyberbezpieczeństwo w ICZMP powołana odrębnym Zarządzeniem Dyrektora ICZMP;
CSIRT NASK	Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym, prowadzony przez Naukową i Akademicką Sieć Komputerową – Państwowy Instytut Badawczy;
Cyberbezpieczeństwo	odporność systemów informacyjnych na działania naruszające

	poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy;
Dokumentacja bezpieczeństwa	zespół powiązanych ze sobą spójnych dokumentów określających zasady i sposoby zarządzania bezpieczeństwem informacji oraz aktywów wspierających przetwarzanie informacji w ICZMP;
Incydent	zdarzenie, które ma lub może mieć niekorzystny wpływ na bezpieczeństwo informacji, ochronę danych osobowych oraz cyberbezpieczeństwo;
Incydent poważny	incydent, który powoduje lub może spowodować poważne obniżenie jakości lub przerwanie ciągłości świadczenia usługi kluczowej. Za incydent poważny będzie uznany incydent, który po szacowaniu ryzyka zostanie określony na poziomie wysoki i bardzo wysoki, zgodnie z BI-3 – Polityką zarządzania ryzykiem;
Informacja (dana)	wszystko, co posiada logiczne znaczenie jako przekaz treści i może być praktycznie wykorzystane w procesach, skutkując osiągnięciem celu. Informacja może być przetwarzana na różnych typach nośników (m.in. papierowych, magnetycznych, optycznych itp), w szczególności w systemach informatycznych;
Informacja objęta tajemnicą przedsiębiorstwa	nieujawnione do wiadomości publicznej informacje techniczne, technologiczne, organizacyjne przedsiębiorstwa lub inne informacje posiadające wartość gospodarczą, co do których przedsiębiorca podjął niezbędne działania w celu zachowania ich poufności;
Informacja publiczna	każda informacja o sprawach publicznych odnosząca się do organu władzy publicznej i dotycząca sfery jego działalności, w tym treść dokumentów, treść wystąpień, opinii i ocen przez nie dokonywanych;
Inspektor Ochrony Danych (IOD)	osoba pełniąca funkcję inspektora ochrony danych w rozumieniu art. 37 RODO wyznaczona przez Dyrektora ICZMP;
Kierownik komórki organizacyjnej	pracownik zajmujący kierownicze stanowisko w ICZMP, jak również kierownika jednostki, oraz bezpośredni przełożony osoby zajmującej samodzielne stanowisko pracy;
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;
Operator usługi kluczowej (OUK)	podmiot, wobec którego Minister Zdrowia wydał decyzję o uznaniu za operatora usługi kluczowej;
Osoba upoważniona	osoba upoważniona przez administratora do przetwarzania danych osobowych, nad którą administrator sprawuje bezpośrednią kontrolę w procesie przetwarzania danych realizowanym przez tę osobę;
OWU NASK	osoba odpowiedzialna za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa, tj. CSIRT NASK, wyznaczona odrębnym Zarządzeniem Dyrektora ICZMP;
Podmiot przetwarzający	osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarzana dane osobowe w imieniu administratora;
Podmiot zewnętrzny	wszyscy pracownicy m.in. wykonawców i kontrahentów, dostawców produktów, materiałów i usług, wykonujących czynności w imieniu i na rzecz ICZMP lub mających dostęp do aktywów ICZMP w związku z realizacją zawartej umowy lub porozumienia;

RODO	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);
Ryzyko	kombinacja prawdopodobieństwa wystąpienia zdarzenia niepożądanego i jego konsekwencje;
System informacyjny	uporządkowany układ odpowiednich elementów, charakteryzujących się pewnymi właściwościami i połączonych wzajemnie określonymi relacjami;
System informatyczny (teleinformatyczny)	zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania zapewniający przetwarzanie, przechowywanie, a także wysyłanie i odbieranie danych przez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego;
UKSC	ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa;
Usługa kluczowa	usługa, która ma kluczowe znaczenie dla utrzymania krytycznej działalności społecznej lub gospodarczej, wymienioną w wykazie usług kluczowych;
VPN (ang. Virtual Private Network, pol. Wirtualna Sieć Prywatna)	technologia umożliwiająca zdalny, szyfrowany dostęp do zasobów i usług sieci teleinformatycznej poprzez sieć publiczną operatora telekomunikacyjnego;
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.

IV. ODPOWIEDZIALNOŚCI I UPRAWNIENIA

I. Zasady ogólne

1. Niniejsza Procedura bezpieczeństwa w relacjach z podmiotami zewnętrznymi określa podstawowe zasady i wymogi w zakresie współpracy z podmiotami zewnętrznymi, w tym współpracy w obszarze dostaw technologii informacyjnych i telekomunikacyjnych.

2. Podmiot zewnętrzny będący stroną zawartej umowy lub porozumienia zobowiązany jest do zapoznania podległych mu pracowników realizujących przedmiot ww. umowy lub porozumienia z zasadami ochrony aktywów informacyjnych ICZMP, określonymi w szczególności w Polityce Bezpieczeństwa Informacji – PP/01 - SZBI i Polityce Ciągłości Działania ICZMP PP/03 - SZBI.

3. Pracownicy podmiotów zewnętrznych, o których powyżej zobowiązani są do przestrzegania wymogów określonych w ww. Politykach.

4. Pracownicy podmiotów zewnętrznych, realizujący określone zadania na podstawie zawartej umowy lub porozumienia mogą otrzymać dostęp do aktywów informacyjnych ICZMP, w tym do:
   1) informacji sklasyfikowanych w poszczególnych grupach:
      a) dane osobowe,
      b) tajemnice prawnie chronione,
      c) tajemnice ICZMP,
      d) informacje jawne,
   2) aktywów wspierających przetwarzanie ww. informacji:
      a) sprzęt (w tym komputery, nośniki informacji),
      b) oprogramowanie,
      c) sieć,
      d) personel ICZMP,
      e) siedziba ICZMP,
      f) organizacja (w tym procedury wewnętrzne określające zasady i tryb funkcjonowania poszczególnych struktur organizacyjnych ICZMP), w ograniczonym zakresie, niezbędnym do realizacji zleconych prac.

5. Przyznawanie, zmiana i odbieranie ww. dostępu do aktywów informacyjnych odbywa się zgodnie z obowiązującymi przepisami prawa, na formalny wniosek właściwego kierownika komórki organizacyjnej, odpowiedzialnego za przygotowanie lub realizację umowy lub porozumienia.

6. Przyznawanie rozszerzonych uprawnień lub dodatkowych przywilejów możliwe jest po przedłożeniu stosownego uzasadnienia przez ww. kierownika i po formalnym odnotowaniu przedmiotowej zmiany.

7. Dostęp zdalny podmiotów zewnętrznych do aktywów informacyjnych ICZMP, np. w związku z wykonywaniem prac serwisowych i aktualizacji, przyznawany jest w zakresie niezbędnym do realizacji zadań i tylko pod nadzorem uprawnionych pracowników ICZMP.

8. Zasady dostępu fizycznego do budynków i pomieszczeń ICZMP dla pracowników podmiotów zewnętrznych:
   1) Pracownicy podmiotów zewnętrznych mają swobodny dostęp do ogólnodostępnej strefy bezpieczeństwa obejmującej wejścia do budynków ICZMP, hole, korytarze oraz wybrane pomieszczenia niestanowiące pomieszczeń ograniczonego dostępu i/lub podwyższonego poziomu bezpieczeństwa, w tym pomieszczenia użyteczności publicznej takie jak punkty obsługi klienta, poczta etc.

   2) Pracownicy podmiotów zewnętrznych mogą uzyskać dostęp do strefy administracyjnej lub strefy medycznej (ograniczonego dostępu), w tym pomieszczeń biurowych, w zakresie wynikającym z

realizacji zadań określonych w treści zawartych umów lub porozumień i na formalny wniosek właściwego kierownika.

3) W strefie o podwyższonym poziomie bezpieczeństwa obejmującej m.in. serwerownie, pracownicy podmiotów zewnętrznych mogą przebywać tylko pod ścisłym nadzorem wybranych pracowników Działu Informatyki. Dostęp do strefy o podwyższonym poziomie bezpieczeństwa jest na bieżąco rejestrowany.

II. Podstawowe zasady bezpieczeństwa i ciągłości działania w zakresie współpracy z podmiotami zewnętrznymi

1. W przypadku korzystania z budynków i pomieszczeń ICZMP, pracownicy podmiotów zewnętrznych zobowiązani są do zapoznania i stosowania się do zapisów obowiązującej instrukcji przeciwpożarowej i przepisów BHP.

2. W uzasadnionych przypadkach mogą być prowadzone dodatkowe szkolenia dla pracowników podmiotów zewnętrznych z zakresu bezpieczeństwa informacji i ciągłości działania.

3. Ww. pracownicy zobowiązani są stale troszczyć się o powierzone im aktywa informacyjne oraz zachować szczególną ostrożność przy bieżącym korzystaniu z tych aktywów, w szczególności zadbać o zabezpieczenie ich przed utratą, kradzieżą, nieuprawnioną modyfikacją, uszkodzeniami mechanicznymi poprzez stosowanie adekwatnych zabezpieczeń.

4. Celem zabezpieczenia aktywów, o których powyżej, pracownicy podmiotów zewnętrznych zobowiązani są do przesyłania plików zawierających informacje chronione (m.in. dane osobowe) z wykorzystaniem sieci Internet, w tym za pośrednictwem poczty elektronicznej, w formie zaszyfrowanej. Zaszyfrowane pliki musza być przesyłane w sposób umożliwiający ich ponowne odszyfrowanie po stronie odbiorcy np. po podaniu unikalnego hasła do pliku. Hasło do zabezpieczonych plików należy przekazać odbiorcy innym kanałem komunikacji od użytego do przesłania danych. Za powyższe czynności odpowiedzialna jest osoba przekazująca dane.

5. Pracownikom podmiotów zewnętrznych nie wolno podejmować prób sprawdzania, testowania i omijania zabezpieczeń powierzonych im aktywów informacyjnych, w tym:
   1) samowolnie modyfikować ustawień związanych z bezpieczeństwem,
   2) świadomie wprowadzać błędnych danych,
   3) podejmować prób przywłaszczenia lub rozszyfrowania informacji uwierzytelniających innych użytkowników.

6. W ramach zapewnienia poufności przetwarzanych informacji , pracownicy podmiotów zewnętrznych zobowiązani są zachować w tajemnicy przez czas nieokreślony (w trakcie jak i po zakończeniu trwania umowy lub porozumienia) informacje udostępnione im w związku z realizacją umowy lub porozumienia oraz chronić je przed ujawnieniem osobom nieuprawnionym.

7. Wymóg zachowania poufności, o którym mowa powyżej obejmuje wszelkie informacje chronione, których ujawnienie mogłoby narazić ICZMP na szkodę. Przedmiotowy wymóg nie dotyczy informacji, które:
   1) są jawne i ogólnodostępne,

2) przekazane zostały podmiotowi zewnętrznemu z możliwością dalszego ujawnienia.

8. W trakcie trwania umowy lub porozumienia, podmiot zewnętrzny zobowiązuje się ponadto:
   1) do wykonania przedmiotu umowy lub porozumienia:
      a) zgodnie z wymogami prawa powszechnie obowiązującego i treścią zawartej umowy lub porozumienia,
      b) z zachowaniem najwyższej profesjonalnej staranności i przy wykorzystaniu całej posiadanej wiedzy i doświadczenia,
      c) przy wsparciu personelu posiadającego niezbędną wiedzę i umiejętności,
      d) w sposób niepowodujący przerwania lub zakłócenia ciągłości pracy ICZMP,
   2) nie zapoznawać się z dokumentami, analizami, zawartością systemu i aplikacji, dysków twardych etc., które nie są związane z przedmiotem umowy lub porozumienia,
   3) nie powielać powierzonych informacji w zakresie szerszym, niż jest to niezbędne dla realizacji przedmiotu umowy lub porozumienia, w tym nie kopiować informacji celem udostępnienia ich osobom nieuprawnionym.

9. Po zakończeniu przedmiotowej współpracy, podmiot zewnętrzny zobowiązany jest niezwłocznie, w zależności od decyzji ICZMP, zwrócić lub zniszczyć udostępnione aktywa, w tym sprzęt lub informacje przekazane mu na dowolnych nośnikach, włączając wszelkie ich kopie. Na pisemne polecenie ICZMP, fakt zwrotu aktywów, w tym informacji potwierdza się w formie pisemnego protokołu przekazania. W przypadku zniszczenia aktywów, podmiot zewnętrzny zobowiązany jest (na polecenie ICZMP) złożyć pisemne oświadczenie potwierdzające przeprowadzenie zniszczenia.

III. Uzyskanie zdalnego dostępu do zasobów sieci ICZMP przez pracowników firm zewnętrznych.

1. Na wniosek Wykonawcy stanowiący załącznik nr 1 do niniejszej procedury, ICZMP udostępni Wykonawcy zdalny dostęp do zasobów sieci teleinformatycznej ICZMP zakresie niezbędnym do prawidłowej realizacji umowy (usługa VPN).

2. Warunkiem uzyskania dostępu do usługi będzie przekazanie ICZMP listy pracowników Wykonawcy uprawnionych do otrzymania dostępu VPN oraz informacji na temat zasobów sieci, do których chce uzyskać dostęp zdalny i które są niezbędne Wykonawcy do należytej realizacji umowy.

3. Wykonawca zobowiązany jest do bezzwłocznego informowania ICZMP o wszelkich zmianach w strukturze organizacyjnej projektu mającej wpływ na zawartość listy pracowników, o której mowa w ust. 2 (np. zwolnienie pracownika).

4. Wykonawca jest zobowiązany do nieujawniania osobom niezaangażowanym w realizację projektu informacji mogących umożliwić uzyskanie dostępu do zasobów sieci teleinformatycznej ICZMP przez osoby niepowołane.

5. Dostęp do zasobów sieci teleinformatycznej jest udzielany na okres trwania umowy lub zobowiązań wynikających z faktu jej zawarcia (np. konieczność świadczenia usługi serwisu gwarancyjnego).

6. ICZMP nie gwarantuje ciągłego działania usługi VPN jednak dołoży on wszelkich starań, aby przerwy w dostępie działania usługi były jak najkrótsze.

7. Brak dostępu zdalnego do zasobów VPN nie będzie powodować żadnych roszczeń Wykonawcy w stosunku do ICZMP, a ponadto nie będzie to zwalniać Wykonawcy z należytego (w szczególności terminowego) wykonania Umowy. W razie wątpliwości poczytuje się, że w przypadku braku dostępu do VPN, jeżeli Wykonawca będzie chciał dotrzymać terminów umownych może wykonywać prace, które dotychczas wykonywał przez VPN, na miejscu w ICZMP.

8. ICZMP przekaże Wykonawcy instrukcję umożliwiającą instalację oraz konfigurację oprogramowania umożliwiającego zdalny dostęp do sieci teleinformatycznej ICZMP.

IV. Zgłaszanie przypadków naruszenia bezpieczeństwa informacji przez podmioty zewnętrzne

1. Osoby i podmioty zewnętrzne wykonujące czynności w imieniu i na rzecz ICZMP lub mające dostęp do aktywów informacyjnych ICZMP, w przypadku zaistnienia okoliczności mogących świadczyć lub świadczących o naruszeniu bezpieczeństwa informacji w ICZMP lub utraty ciągłości działania, zobowiązani są niezwłocznie poinformować o szczegółach i charakterze zdarzenia kierownika Centralny Zespół ds. Reagowania na Incydenty (CZRI).

2. Zgłoszenie, o którym mowa powyżej, należy przesłać drogą mailową na adres incydent@iczm.edu.pl, podając dane kontaktowe, okoliczności oraz czas wystąpienia zdarzenia, wskazującego na naruszenie lub próbę naruszenia (można skorzystać z Formularza zgłoszenia naruszenia bezpieczeństwa informacji i ciągłości działania, którego wzór stanowi załącznik nr 2 do niniejszej Procedury).

3. Próby lub przypadki nieautoryzowanego dostępu do aktywów informacyjnych ICZMP są identyfikowane jako incydenty związane z bezpieczeństwem informacji.

4. Po powzięciu informacji o okolicznościach mogących świadczyć lub świadczących o naruszeniu bezpieczeństwa informacji lub utracie ciągłości działania, dalsze postępowanie, w tym obsługa i wyjaśnienie przyczyn incydentu związanego z bezpieczeństwem informacji, odbywa się zgodnie z Polityką zarządzania incydentem (BI-4-U).

5. Naruszenie postanowień umowy, porozumienia lub wymogów obowiązującej dokumentacji bezpieczeństwa i ciągłości działania przez podmiot zewnętrzny stanowi podstawę do odstąpienia od umowy lub porozumienia i żądania pokrycia powstałej szkody lub zapłaty kary umownej, jeżeli taki obowiązek wynikał z zawartej umowy lub porozumienia.

6. Z tytułu działań podmiotów zewnętrznych i jego przedstawicieli, niezgodnych z przepisami prawa powszechnie obowiązującego (w tym dot. niewłaściwego przetwarzania danych osobowych), grożą odrębne kary określone w szczególności w:
   1) kodeksie pracy,
   2) kodeksie cywilnym,
   3) kodeksie karnym,
   4) RODO oraz ustawie o ochronie danych osobowych.

V. DOKUMENTY ZWIĄZANE:

1. PP/01 – SZBI - Polityka bezpieczeństwa informacji;
2. PP/02 – SZBI - Polityka ochrony danych osobowych;
3. PP/03 – SZBI - Polityka ciągłości działania;
4. PP/04 – SZBI - Procedura nadawania upoważnień;
5. PP/05 – SZBI - Procedura udostępniania danych;
6. PP/06 – SZBI - Procedura powierzenia przetwarzania danych;
7. PP/07 – SZBI - Procedura oceny skutków;
8. PP/08 – SZBI - Procedura zarządzania ryzykiem bezpieczeństwa informacji;
9. PP/09 – SZBI - Procedura zarządzania podatnościami;
10. PP/10 – SZBI - Procedura zarządzania incydentami związanymi z bezpieczeństwem informacji;
11. PP/11 – SZBI - Procedura użytkowania sieci teleinformatycznej;
12. PP/12 – SZBI - Procedura rejestracji i inwentaryzacji oprogramowania i sprzętu komputerowego;
13. PP/13 – SZBI - Procedura pracy zdalnej;
14. PP/14 – SZBI - Procedura dostępu VPN do zasobów sieci ICZMP;
15. PP/15 – SZBI - Procedura przechowywania i przekazywania hasła administratora systemu;
16. PP/16 – SZBI - Procedura wykonywania kopii zapasowych;
17. PP/17 – SZBI - Procedura rejestracji i inwentaryzacji sprzętu medycznego;
18. PP/18 – SZBI - Procedura zarządzania zmianą IT;
19. PP/19 – SZBI - Procedura privacy by design, privacy by default;
20. PP/20 – SZBI - Procedura zarządzania aktywami informacyjnymi;
21. PP/21 – SZBI - Procedura zarządzania bezpieczeństwem zasobów ludzkich;
22. PP/22 – SZBI - Procedura bezpieczeństwa fizycznego i środowiskowego;
23. PP/23 – SZBI - Procedura zarządzania kluczami;
24. PP/24 – SZBI - Procedura zarządzania uprawnieniami w systemie kontroli dostępu;
25. PP/25 – SZBI - Procedura dostępu do serwerowni;
26. PP/26 – SZBI - Procedura zarządzania systemem monitoringu wizyjnego;
27. PP/27 – SZBI - Procedura korzystania z bezprzewodowej sieci dla pracownika;
28. PP/28 – SZBI - Procedura korzystania z bezprzewodowej sieci dla gości;
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:

1. Załącznik nr 1 do Procedury PP/29 – SZBI - Wniosek o utworzenie konta VPN i udzielenie dostępu do zasobów sieciowych pracowników Wykonawcy (firm zewnętrznych);
2. Załącznik nr 2 do Procedury PP/29 – SZBI - Formularza zgłoszenia naruszenia bezpieczeństwa informacji i ciągłości działania.

Załącznik nr 1 do Procedury PP/29 – SZBI - Wniosek o utworzenie konta VPN i udzielenie dostępu do zasobów sieciowych pracowników Wykonawcy (firm zewnętrznych)

WNIOSEK ZBIOROWY O UTWORZENIE, PRZEDŁUŻENIE WAŻNOŚCI LUB USUNIĘCIE KONTA VPN dla personelu Wykonawcy (firmy zewnętrznej)

Wniosek dotyczy:					
Utworzenia konta VPN:		*Przedłużenia ważności konta VPN*		*Usunięcia konta VPN*	
Wnioskujący:					
Firma:					
Adres siedziby firmy / pieczęć firmowa:					
Adres służbowej poczty elektronicznej:					
Numer umowy, do realizacji której niezbędny jest dostęp VPN:					
Termin obowiązywania umowy:					
Lista pracowników uprawnionych do połączenia VPN					
Imię i nazwisko pracownika	E-mail pracownika		Numer telefonu pracownika	Grupa uprawnień	
Wnioskujący (imię i nazwisko)					
ICZMP					
ZGODA					
Wniosek akceptuję / odrzucam					

Data nadania dostępu :	
Zakres nadawanych uprawnień	

Potwierdzenie nadania / odebrania uprawnień:	

Załącznik nr 2 do Procedury PP/29 – SZBI - Formularza zgłoszenia naruszenia bezpieczeństwa informacji i ciągłości działania

Formularz zgłoszenia zdarzenia	
Data zgłoszenia:	
Dane kontaktowe osoby zgłaszającej zdarzenie	
Imię i nazwisko	
Dział / firma	
Numer telefonu	
Adres e-mail	
Miejsce wystąpienia zdarzenia	
Opis zdarzenia	
Zasób, którego dotyczy zdarzenie	
Data i godzina zdarzenia	
Inne	
Podejrzewana przyczyna wystąpienia zdarzenia	
Działania zabezpieczające podjęte bezpośrednio po wystąpieniu zdarzenia / sposób zabezpieczenia dowodów	
Zaobserwowane skutki zdarzenia. Szkody spowodowane przez incydent	
Osoby poinformowane o wystąpieniu zdarzenia	
Data / godzina zaobserwowania zdarzenia	