Załącznik nr 1
do Zarządzenia nr 142/2022 Dyrektora
Międzyleskiego Szpitala Specjalistycznego w Warszawie

Polityka bezpieczeństwa w relacjach z podmiotami zewnętrznymi

OPRACOWAŁ	WŁAŚCICIEL PROCEDURY
ODO Consulting sp. z o.o.	Kierownik Działu Zamówień Publicznych
Data i podpis:	Data i podpis:
SPRAWDZIŁ	**ZATWIERDZIŁ**
Marzena Dymkowska-Gacyk Zastępca Dyrektor ds. Administracyjno-Eksploatacyjnych	dr Jarosław Rosłon Dyrektor
Data i podpis:	Data i podpis:

Polityka bezpieczeństwa w relacjach z podmiotami zewnętrznymi stanowi dokument I poziomu SZBI.

Relacje Szpitala z podmiotami zewnętrznymi mają charakter sformalizowany, a współpraca odbywa się w oparciu o obowiązujące przepisy prawa, Politykę Bezpieczeństwa Informacji, niniejszą Politykę oraz indywidualne umowy i porozumienia.

Rejestry zawartych umów prowadzony jest centralnie przez Sekretariat Szpitala.

Celem zapewnienia ochrony aktywów informacyjnych udostępnianych podmiotom zewnętrznym wykonującym czynności w imieniu i na rzecz Szpital lub mającym dostęp do aktywów Szpitala oraz utrzymania ciągłości realizacji usług świadczonych przez ww. podmioty, wprowadza się niniejsze zasady i wymogi bezpieczeństwa i ciągłości działania.

Przedmiotowe zasady i wymogi dot. w szczególności:

1) udostępniania aktywów informacyjnych oraz monitorowania i kontroli dostępu,
2) przestrzegania określonych zasad i wymogów przez podmioty zewnętrzne,
3) obowiązków podmiotów zewnętrznych w zakresie zapewnienia ochrony aktywów informacyjnych Szpitala i ciągłości świadczonych usług,
4) zgłaszania przypadków naruszenia lub podejrzenia naruszenia bezpieczeństwa informacji lub ciągłości działania,
5) uświadamiania pracowników podmiotów zewnętrznych w zakresie bezpieczeństwa informacji i ciągłości działania,
6) postępowania z poufnymi informacjami, w tym powierzonymi podmiotom zewnętrznym danymi osobowymi,
7) dodatkowych wymogów w zakresie utrzymania ciągłości realizacji procesów krytycznych.

Jednocześnie zapisy niniejszej Polityki stanowią punkt wyjścia do indywidualnych ustaleń i zapisów uzupełniających w umowach lub porozumieniach z podmiotami zewnętrznymi, których zakres zależy od charakteru i specyfiki współpracy.

W przypadku wykonywania zadań delegowanych lub korzystania z aktywów, w tym przetwarzania informacji powierzonych przez podmioty zewnętrzne w drodze stosownej umowy lub porozumienia, poza wymogami określonymi w obowiązującej w Szpitalu dokumentacji bezpieczeństwa i ciągłości działania, dopuszcza się stosowanie dodatkowych wymogów określonych przez ww. podmioty zewnętrzne, o ile wskazane wymogi nie obniżają

poziomu bezpieczeństwa pozostałych informacji przetwarzanych w Szpitalu i nie generują ryzyka utraty ciągłości działania Szpitala.

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

Niniejsza Polityka bezpieczeństwa w relacjach z podmiotami zewnętrznymi podlega przeglądom pod kątem aktualności, przydatności i adekwatności, zgodnie z zasadami monitorowania i aktualizacji dokumentacji bezpieczeństwa i ciągłości działania określonymi w Polityce monitorowania i nadzoru nad bezpieczeństwem informacji i ciągłością działania.

Użyte w niniejszej Polityce pojęcia mają następujące znaczenie:

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 Szpital;
Aktywa	wszystko, co ma wartość dla Szpitala, a w szczególności: personel, wizerunek, informacje wytwarzane, przetwarzane i przechowywane w Szpitalu, mienie wykorzystywane przez Szpital 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 Szpitala i wymagające właściwej ochrony przed utratą dostępności, poufności i integralności;
Analiza ryzka	zidentyfikowane ryzyka należy poddać analizie mającej na celu określenie prawdopodobieństwa wystąpienia danego ryzyka i możliwych jego skutków;
Audyt	systematyczny, niezależny i udokumentowany proces uzyskiwania dowodu z audytu oraz jego obiektywnej oceny w celu określenia stopnia spełnienia kryteriów audytu;
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 Szpitala;
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 Szpitalu;
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 Szpitala;
Kierownik komórki organizacyjnej	pracownik zajmujący kierownicze stanowisko w Szpitalu, 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 Szpitala;
Pełnomocnik ds. SZBI	osoba odpowiedzialna za bezpieczeństwo informacji w Szpitalu wyznaczona odrębnym Zarządzeniem Dyrektora Szpitala;
Personel Szpitala	osoba zatrudniona przez Szpital na podstawie umowy o pracę oraz osoba świadcząca na rzecz Szpitala usługi na podstawie umów cywilnoprawnych, a także praktykanci, wolontariusze, stażyści i studenci;
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 Szpital lub mających dostęp do aktywów Szpitala w związku z realizacją zawartej umowy lub porozumienia;
Poufność	właściwość, że informacja nie jest udostępniana lub wyjawiana nieupoważnionym osobom, podmiotom lub procesom;
Przetwarzanie danych osobowych	operacja lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;
Przetwarzanie informacji	jakiekolwiek operacje wykonywane na informacjach obejmujące ich zbieranie, gromadzenie, utrwalanie, przechowywanie, opracowywanie, zmienianie, wytwarzanie, udostępnianie, przekazywanie i usuwanie;
PUODO	niezależny organ publiczny powołany w celu ochrony podstawowych praw i wolności osób fizycznych w związku z przetwarzaniem oraz ułatwiania swobodnego przepływu danych w Unii Europejskiej, zgodnie z art. 51 RODO, tj. Prezes Urzędu Ochrony Danych Osobowych;
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;
Szpital	Międzyleski Szpital Specjalistyczny w Warszawie;
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;
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.

I. Zasady ogólne

1. Niniejsza Polityka 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 Szpitala, określonymi w szczególności w Polityce Bezpieczeństwa Informacji (BI-1-P) i Polityce Ciągłości Działania Szpitala (BI-6-P).

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 Szpitala, w tym do:
   1) informacji sklasyfikowanych w poszczególnych grupach:
      a) dane osobowe,
      b) tajemnice prawnie chronione,
      c) tajemnice Szpitala,
      d) informacje jawne,
   2) aktywów wspierających przetwarzanie ww. informacji:
      a) sprzęt (w tym komputery, nośniki informacji),
      b) oprogramowanie,
      c) sieć,
      d) personel Szpitala,
      e) siedziba Szpitala,
      f) organizacja (w tym procedury wewnętrzne określające zasady i tryb funkcjonowania poszczególnych struktur organizacyjnych Szpitala), 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 Szpitala, np. w związku z wykonywaniem prac serwisowych i aktualizacji, przyznawany jest w zakresie niezbędnym do realizacji zadań i tylko pod nadzorem uprawnionych pracowników Szpitala.

8. Zasady dostępu fizycznego do budynków i pomieszczeń Szpital dla pracowników podmiotów zewnętrznych:
   1) Pracownicy podmiotów zewnętrznych mają swobodny dostęp do ogólnodostępnej strefy bezpieczeństwa obejmującej wejścia do budynków Szpital, 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 Szpital, 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 Szpital 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 Szpitala,

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

III. Treść umów i porozumień z podmiotami zewnętrznymi

1. Celem ograniczenia ryzyka związanego z dostępem podmiotów zewnętrznych do aktywów Szpital lub utratą ciągłości działania Szpitala, w treści zawieranych umów lub porozumień wprowadza się niezbędne wymogi dot. bezpieczeństwa aktywów informacyjnych lub utrzymania ciągłości świadczonych usług, do których przestrzegania w trakcie i po zakończeniu umowy lub porozumienia zobowiązany jest ww. podmiot zewnętrzny.

2. Podstawowy zakres wymogów, o których mowa powyżej wynika wprost z obowiązujących przepisów prawa oraz dokumentacji bezpieczeństwa i ciągłości działania, w szczególności Polityki bezpieczeństwa informacji i Polityki ciągłości działania Szpitala.

3. Właściwy kierownik komórki organizacyjnej, odpowiedzialny za przygotowanie lub realizację umowy lub porozumienia, przygotowuję adekwatne zapisy dot. bezpieczeństwa informacji lub ciągłości działania.

4. Zakres oraz stopień szczegółowości zapisów dot. bezpieczeństwa informacji lub ciągłości działania w treści umowy lub porozumienia zależy od przedmiotu i specyfiki podejmowanej współpracy oraz zidentyfikowanych zagrożeń.

5. Poza standardowymi wymogami wprost określonymi w obowiązujących przepisach prawa oraz dokumentacji bezpieczeństwa i ciągłości działania, dodatkowe zapisy dot. bezpieczeństwa informacji i ciągłości działania mogą uwzględniać np.:
   1) cel i zakres przetwarzanych informacji,
   2) wykaz osób upoważnionych do wymiany informacji i listę zatwierdzonych narzędzi do komunikacji,
   3) zakres i poziom świadczonych usług,
   4) zasady i tryb postępowania w przypadku awarii lub katastrofy (maksymalny czas reakcji, maksymalny czas naprawy) i zapewnienia ciągłości świadczenia usług i dostaw,
   5) akceptowalny poziom dostępności świadczonych usług,
   6) ochronę własności intelektualnej i praw autorskich.

6. Przy zawieraniu umów z kluczowymi dostawcami usług lub produktów, niezbędnych do realizacji procesów krytycznych, tam gdzie to uzasadnione należy uwzględnić w treści umowy dodatkowe zapisy dot. utrzymania ciągłości działania i świadczenia usług na rzecz Szpital dot.:
   1) ustanowienia po stronie dostawców Planów ciągłości działania z czasami nie dłuższymi niż czasy docelowego wznowienia działania zidentyfikowane dla danego procesu krytycznego,
   2) wykonywania przynajmniej raz do roku testów Planów ciągłości działania przez dostawcę,
   3) ich ewentualnego uczestnictwa w testach ciągłości działania realizowanych przez Szpital,
   4) umożliwienia przeprowadzenia audytów Planu ciągłości działania u dostawcy.
   5) W przypadku korzystania przez dostawcę z usług podwykonawców wymogi określone w pkt 1-4 dotyczą również podwykonawców.

7. Dodatkowo, w przypadku powierzenia podmiotom zewnętrznym przetwarzania danych osobowych, ww. kierownik właściwej komórki organizacyjnej Szpital przygotowuje stosowne zapisy dotyczące ochrony danych osobowych (umowa powierzenia), zgodnie z Polityką ochrony danych osobowych (BI-2-U).

8. Przy okazji doskonalenia dostarczanych produktów i usług, zmiany wynikające m.in. z wprowadzenia nowych wersji dokumentacji bezpieczeństwa i ciągłości działania,

wprowadzenia nowych zabezpieczeń, zmiany lokalizacji, należy - tam gdzie to niezbędne - uwzględnić w formie aneksów do już istniejących umów lub porozumień.

9. Przykładowe standardowe zapisy dot. bezpieczeństwa informacji i ciągłości działania w umowach lub porozumieniach z podmiotami zewnętrznymi określa załącznik nr 1 do niniejszej Polityki.

IV. Monitorowanie i przegląd usług świadczonych przez podmioty zewnętrzne

1. Dostęp podmiotów zewnętrznych i korzystanie z aktywów informacyjnych Szpitala przez ich pracowników są nadzorowane i monitorowane, m.in. za pośrednictwem systemu monitoringu wizyjnego.

2. Bieżący nadzór nad udostępnianiem i korzystaniem przez podmioty zewnętrzne z aktywów informacyjnych Szpital prowadzi właściwy kierownik komórki organizacyjnej lub osoba przez niego wyznaczone.

3. Ww. osoby zobowiązane są również do monitorowania czy współpracujące podmioty zewnętrzne realizują swoje zadania zgodnie z prawem i treścią zawartych umów lub porozumień, a dostarczane przez nich produkty i usługi są zgodne z przedmiotem umowy lub porozumienia oraz spełniają oczekiwania odbiorców.

4. Na wniosek Szpital, podmiot zewnętrzny zobowiązany jest przekazać informacje dotyczące postępów prac, przyczyn opóźnień lub nienależytego wykonywania zawartej umowy lub porozumienia. Informacje przekazywane są niezwłocznie w formie pisemnej.

5. W uzasadnionych przypadkach, podmiot zewnętrzny zobowiązany jest umożliwić weryfikację postępów prac bezpośrednio w swojej siedzibie w trybie postępowania sprawdzającego (audytu bezpieczeństwa).

6. Przedmiotowe zapisy dot. monitorowania i przeglądu usług świadczonych przez podmioty zewnętrzne mogą zostać doszczegółowione w treści zawartych umów lub porozumień (ewentualnie w aneksach do już istniejących umów lub porozumień).

V. Zgłaszanie przypadków naruszenia bezpieczeństwa informacji przez podmioty zewnętrzne

1. Osoby i podmioty zewnętrzne wykonujące czynności w imieniu i na rzecz Szpital lub mające dostęp do aktywów informacyjnych Szpitala, w przypadku zaistnienia okoliczności mogących świadczyć lub świadczących o naruszeniu bezpieczeństwa informacji w Szpitalu 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@mssw.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 Polityki).

3. Próby lub przypadki nieautoryzowanego dostępu do aktywów informacyjnych Szpitala 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.

IV. Zasady współpracy z podmiotami zewnętrznymi w przypadku naruszenia bezpieczeństwa informacji

1. Poza współpracą z tytułu zawartych umów i porozumień, z uwagi na wymogi prawa powszechnie obowiązującego, celem zapewnienia kompleksowej ochrony przetwarzanych informacji i utrzymania ciągłości działania Szpitala, w tym ochrony przed cyberzagrożeniami, wymiany wiedzy i doświadczeń oraz wsparcia procesu zarządzania zdarzeniami, w tym incydentami związanymi z bezpieczeństwem informacji i ciągłością działania, pracownicy Szpital współpracują z wybranymi instytucjami, organizacjami oraz podmiotami sektora publicznego i prywatnego.

2. W ramach przedmiotowej współpracy, w uzasadnionych przypadkach, w szczególności:
   1) w przypadku wybranych incydentów o priorytecie wysokim i bardzo wysokim,
   2) w przypadku incydentów, które powodują lub mogą spowodować obniżenie jakości lub przerwanie realizacji zadania realizowanego przez Szpital,
   3) w przypadku incydentów noszących znamiona przestępstwa,

   - informacja o incydencie przekazywana jest do właściwych podmiotów zewnętrznych, w tym:
      a) organów ścigania w przypadku incydentów wyczerpujących znamiona przestępstwa (np. przestępstwa przeciwko ochronie informacji wskazane w Kodeksie Karnym),
      b) Agencji Bezpieczeństwa Wewnętrznego,
      c) właściwych zespołów reagowania na incydenty bezpieczeństwa komputerowego – w tym CSIRT NASK.

3. Współpraca z organem nadzorczym - Prezesem Urzędu Ochrony Danych Osobowych prowadzona jest w obszarze ochrony danych osobowych, w tym wymiany doświadczeń i stałego podnoszenia wiedzy pracowników Szpitala.

4. Przypadki naruszenia ochrony danych osobowych prowadzącego do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych są niezwłocznie zgłaszane organowi nadzorczemu (Prezesowi UODO), na zasadach i w trybie szczegółowo określonym w obowiązującej w Szpital Polityce zarządzania incydentem (BI-4-U).

Załączniki:

1. Przykładowe standardowe zapisy dot. bezpieczeństwa informacji i ciągłości działania w umowach lub porozumieniach z podmiotami zewnętrznymi;
2. Formularza zgłoszenia naruszenia bezpieczeństwa informacji i ciągłości działania.

Dokumenty powiązane I poziomu SZBI:

1. BI-1-P – Polityka Bezpieczeństwa Informacji;
2. BI-6-P – Polityka ciągłości działania;

Dokumenty powiązane II poziomu SZBI:

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

Dokumenty powiązane III poziomu SZBI:

10. BI-2-1-U – Procedura nadawania upoważnień;
11. BI-2-2-U – Procedura udostępniania danych;
12. BI-2-3-U – Procedura udostępniania uczelni dokumentacji medycznej;
13. BI-2-4-U – Procedura powierzenia przetwarzania danych;
14. BI-2-5-Z – Procedura oceny skutków;
15. BI-3-1-U – Procedura zarządzania podatnościami;
16. BI-3-2-U – Procedura działań korygujących i doskonalących;
17. BI-5-1-U – Procedura rejestracji i inwentaryzacji oprogramowania i sprzętu komputerowego;
18. BI-5-2-U – Procedura pracy zdalnej;
19. BI-5-3-U – Procedura dostępu VPN do zasobów sieci Szpitala;
20. BI-5-4-Z – Procedura przechowywania i przekazywania hasła ASI;
21. BI-5-5-Z – Procedura wykonywania kopii zapasowych;
22. BI-5-6-U – Procedura rejestracji i inwentaryzacji sprzętu medycznego;
23. BI-5-7-Z – Procedura zarządzania zmianą IT;

24. BI-5-8-Z – Procedura privacy by design, privacy by default;
25. BI-6-1-U – Plan ciągłości działania;
26. BI-7-1-U – Procedura zarządzania bezpieczeństwem osobowym;
27. BI-8-1-U – Procedura zarządzania kluczami;
28. BI-8-2-U – Procedura zarządzania uprawnieniami w systemie kontroli dostępu;
29. BI-8-3-Z – Procedura wykonywania przeglądu systemów;
30. BI-8-4-Z – Procedura dostępu do serwerowni;
31. BI-8-5-Z – Procedura zarządzania systemem monitoringu wizyjnego;
32. BI-8-7-U – Procedura korzystania z bezprzewodowej sieci dla pracownika;
33. BI-8-8-Z – Procedura dostępu do sejfów i szaf metalowych;
34. BI-10-1-U – Procedura audytów wewnętrznych SZBI.

Dokumenty związane:

1. Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa;
2. Ustawa z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta;
3. Ustawa z dnia z dnia 15 kwietnia 2011 r. o działalności leczniczej;
4. Ustawa z dnia 22 sierpnia 1997 r. o ochronie osób i mienia;
5. Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne;
6. 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;
7. 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;
8. 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).

Załącznik nr 1 do Polityki bezpieczeństwa w relacjach z podmiotami zewnętrznymi

Przykładowe standardowe zapisy dot. bezpieczeństwa informacji i ciągłości działania w umowach lub porozumieniach z podmiotami zewnętrznymi

§ … BEZPIECZEŃSTWO INFORMACJI i CIĄGŁOŚĆ DZIAŁANIA

1. W związku z realizacją niniejszej Umowy/Porozumienia*, Zleceniobiorca/Wykonawca/Podmiot zewnętrzny* będący stroną zawartej Umowy/Porozumienia* zobowiązany jest do zapewnienia bezpieczeństwa informacji przetwarzanych w związku jej/jego* realizacją, ochrony pozostałych udostępnionych mu aktywów Szpitala/Zamawiającego, wspierających przetwarzanie tych informacji, w szczególności do zapewnienia ich poufności, integralności oraz dostępności oraz do zapewnienia ciągłości realizacji usług świadczonych na rzecz Szpitala.
2. Ww. Zleceniobiorca/Wykonawca/Podmiot zewnętrzny* zobowiązuje się do wykonania przedmiotu Umowy/Porozumienia* zgodnie z przepisami prawa powszechnie obowiązującego oraz do zapoznania się przed jej podpisaniem i przestrzegania wymogów w zakresie bezpieczeństwa informacji i ciągłości działania określonych w Polityce Bezpieczeństwa Informacji (BI-1-P) i Polityce Ciągłości Działania Szpitala (BI-6-P), dostępnych na stronie internetowej Szpitala w zakładce „Bezpieczeństwo informacji”.
3. Podmiot, o którym mowa w ust. 1 i 2, w ramach niniejszej Umowy/Porozumienia* zobowiązuje się w szczególności:
   1) stale troszczyć się o powierzone mu informacje i aktywa wspierające ich przetwarzanie oraz zachować szczególną ostrożność przy bieżącym korzystaniu z tych aktywów, w tym zadbać o zabezpieczenie ich przed utratą, kradzieżą, nieuprawnionym udostępnieniem, nieuprawnioną modyfikacją, uszkodzeniami mechanicznymi,
   2) korzystać z powierzonych mu informacji i aktywów wspierających ich przetwarzanie, zgodnie z oraz wyłącznie do celów wynikających z zapisów zawartej Umowy/Porozumienia*,
   3) przesyłać informacje chronione z wykorzystaniem sieci Internet w formie zaszyfrowanej,
   4) nie powielać, w tym nie kopiować informacji chronionych, udostępnionych i opracowanych w trakcie Umowy/Porozumienia* w zakresie szerszym, niż jest to potrzebne do jej/jego* realizacji,
   5) informować Zamawiającego o każdym podejrzeniu naruszeniu bezpieczeństwa informacji i/ lub utraty ciągłości działania Szpitala,
   6) niezwłocznie po zakończeniu niniejszej Umowy/Porozumienia*, trwale usunąć lub zniszczyć informacje chronione przetwarzane w ramach jej/jego* realizacji, chyba że

obowiązek ich dalszego przetwarzania wynika wprost z przepisów prawa powszechnie obowiązującego.

4. Jednocześnie Zleceniobiorca/Wykonawca/Podmiot zewnętrzny* potwierdza, że pracownicy bezpośrednio realizujący przedmiot niniejszej Umowy/Porozumienia* zostali zapoznani i zobowiązani do przestrzegania przedmiotowych wymogów w zakresie bezpieczeństwa informacji i ciągłości działania.

Załącznik nr 2 do Polityki bezpieczeństwa w relacjach z podmiotami zewnętrznymi

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	