Podstawowe wymagania dotyczące bezpieczeństwa informacji dla Podmiotów Zewnętrznych

Załącznik zawiera podstawowe wymagania z zakresu bezpieczeństwa informacji, które winny być spełnione przez Podmiot Zewnętrzny (jeśli dotyczy) współpracujący z Centrum Onkologii im. prof. F. Łukaszczyka w Bydgoszczy (zwanego dalej Centrum). Uregulowania szczegółowe powinny stanowić zapisy zawartej umowy współpracy.

Centrum Onkologii im. prof. F. Łukaszczyk w Bydgoszczy wdrożyło i certyfikowało wymagania normy ISO 27001, zobowiązuje się zatem przedstawicieli Podmiotów Zewnętrznych do przestrzegania podczas współpracy z Centrum obowiązujących Polityk bezpieczeństwa.

1) Niniejsze wymagania powstały w celu zapewnienia ochrony aktywów organizacji, które udostępnione zostały podmiotom zewnętrznym współpracującym z Centrum.
2) Wymagania z zakresu bezpieczeństwa informacji dotyczą Podmiotów Zewnętrznych, które uzyskały dostęp, możliwość jej przetwarzania, przechowywania, przesyłania lub dostarczania elementów infrastruktury teleinformatycznej celem przetwarzania informacji należących do Centrum.
3) Przetwarzanie informacji należących do Centrum przez Podmioty Zewnętrzne musi odbywać się z uwzględnieniem klasyfikacji informacji uwzględnionej w tabeli tab. nr 1.

Atrybut	Opis	Zabezpieczanie		
		Wersja ustna	Wersja elektroniczna	Wersja papierowa / nośniki danych
Publicznie dostępne	Informacje dostępne dla wszystkich pracowników Podmiotu zewnętrznego, w skład których wchodzą informacje publicznie dostępne, uzyskane z niezależnych w stosunku do Centrum Onkologii źródeł.	Informacje Publiczne nie muszą być w żaden specjalny sposób zabezpieczane.		
Jawne dla użytkowników informacji	Informacje dostępne tylko dla pracowników Podmiotu zewnętrznego mających kontakt z informacjami należącymi do Centrum Onkologii w ramach pełnionych obowiązków, w skład których wchodzą wszystkie informacje nie zaliczone do kategorii Publicznie dostępne lub chronione – większość informacji	Należy poinformować odbiorcę o charakterze informacji. Informacje należy przekazywać w sposób uniemożliwiający usłyszenie informacji przez osoby postronne	Należy zapisywać dokumenty na dysku szyfrowanym, przekazywać mailowo w formie zahasłowanej Kopia dokumentów powinna być umieszczona w bezpiecznej sieci komunikacji wewnętrznej Podmiotu Zewnętrznego, do której dostawcy posiadają odpowiednie uprawnieni	Zakaz wynoszenia poza miejsce ustalone jako miejsce realizacji zleconych prac.
Chronione	Dostępne tylko dla upoważnionych pracowników Podmiotu Zewnętrznego, w skład których wchodzą: dane stanowiące tajemnicę zawodową, dane osobowe klientów/pracowników/pacjentów,	Należy poinformować odbiorcę o charakterze informacji. Informacje należy przekazywać w sposób uniemożliwiający usłyszenie informacji przez osoby postronne	Należy zapisywać dokumenty na dysku szyfrowanym. Przesyłanie informacji przy użyciu poczty szyfrowanej wyłącznie do upoważnionych pracowników.	Zakaz wynoszenia poza miejsce ustalone jako miejsce realizacji zleconych prac. Przechowywanie informacji w szafach/szafkach pod kluczem.

Podstawowe wymagania dotyczące bezpieczeństwa informacji dla Podmiotów Zewnętrznych

4) Bezpieczeństwo informacji – Podmiot Zewnętrzny winien zapewnić, że wszystkie osoby mające dostęp do informacji chronionych podpisały klauzule poufności oraz zostały przeszkolone w zakresie bezpieczeństwa informacji.
5) Bezpieczeństwo personelu – Podmiot Zewnętrzny winien zapewnić bezpieczeństwo wykorzystywanego personelu adekwatnie do zadań realizowanych na rzecz Centrum Onkologii:
    a) przekazanie swojemu personelowi realizującemu zadania na rzecz Centrum informacji o wymaganiach bezpieczeństwa współpracy,
    b) podpisanie przez pracowników realizujących zadania na rzecz Centrum oświadczeń zawierającą klauzulę o zachowaniu poufności oraz o zapoznanie z obowiązującymi wymaganiami prawnymi z zakresu bezpieczeństwa informacji i ochrony danych osobowych.
6) Bezpieczeństwo powierzonych aktywów - Podmiot Zewnętrzny winien zapewnić bezpieczeństwo wymiennych nośników danych wykorzystywanych w związku z realizacją zadań na rzecz Centrum. W szczególności wymaganym jest aby:
    a) Użytkownicy aktywów posiadali świadomość odnośnie bezpiecznego korzystania z udostępnionych aktywów,
    b) Po zakończeniu realizacji zleconych zadań użytkownicy zwrócili aktywa lub w przypadku gdy są to dane usunęli je w skuteczny sposób.
7) Praca na odległość – dostęp pracowników Podmiotu Zewnętrznego z sieci publicznych do systemów IT Centrum może być realizowany wyłącznie przy użyciu metod kryptograficznych takich jak VPN (uregulowania szczegółowe zawarte w umowie współpracy - jeśli dotyczy). Podmiot Zewnętrzny winien zapewnić bezpieczeństwo pracy zdalnej a w szczególności:
    a) zdalny dostęp do zasobów Centrum musi być wykorzystywany tylko w celach i zakresie określonym przez Centrum,
    b) zdalny dostęp nadawany jest imiennie i wydawany każdemu pracownikowi Podmiotu Zewnętrznego indywidualnie,
    c) osoby korzystające ze zdalnego dostępu są zobowiązane do zapewnienia ochrony fizycznej zasobów oraz zachowania poufności informacji niezbędnych do korzystania ze zdalnego dostępu,
    d) osoby korzystające z zasobów oraz informacji niezbędnych do korzystania ze zdalnego dostępu nie mogą ich udostępniać ani ujawniać innym osobom,
    e) zabronione jest wykorzystywanie podatności w zdalnym dostępie zidentyfikowanych przez osoby korzystające ze zdalnego dostępu,
    f) wszelkie wykryte podatności muszą być niezwłocznie zgłoszone Kierownikowi Działu Zarządzania i Informatyzacji Centrum. Dalsze korzystanie ze zdalnego dostępu winno być realizowane wyłącznie po wyrażeniu zgody przez Centrum,
    g) osoby korzystające ze zdalnego dostępu muszą zapewnić, że zdalny komputer posiada zainstalowane aktualne oprogramowanie chroniące przed złośliwym kodem,
    h) Centrum Onkologii ma prawo do nagrywania, przechowywania i wykorzystywania w celach dowodowych nagrań z przeprowadzonego zdalnego dostępu,
    i) Centrum Onkologii ma prawo do rejestrowania, przechowywania i wykorzystywania w celach dowodowych wszelkich zdarzeń związanych z realizacją zdalnego dostępu.

Podstawowe wymagania dotyczące bezpieczeństwa informacji dla Podmiotów Zewnętrznych

8) Urządzenia przenośne – przyjęta została w Centrum Polityka stosowania urządzeń pamięci masowej USB, która wprowadza ograniczenia w ich stosowaniu. W Centrum Onkologii dokonuje się szyfrowania Urządzeń pamięci USB obligatoryjnie. W przypadku konieczności zastosowania na potrzeby działań serwisowych innych urządzeń USB nie podlegających zasadom nadzoru obowiązujących w Centrum fakt ten Podmiot Zewnętrzny winien zgłosić pisemnie Kierownikowi Działu Zarządzania i Informatyzacji.
9) Dostęp do zasobów - dostęp do zasobów Centrum dla Podmiotu Zewnętrznego powinien być określony i usankcjonowany z zachowaniem następujących wymagań:
   a. uprawnienia do systemów dla pracowników Podmiotu Zewnętrznego nadawane są zgodnie z obowiązującymi w Centrum procedurami ZSZ, konieczność nadania dostępu do systemów winna zostać zgłoszona do Działu Zarządzania i Informatyzacji,
   b. przedzielanie uprawnień musi być zgodne z „zasadą wiedzy koniecznej" co oznacza, że pracownicy Podmiotu Zewnętrznego mogą otrzymać taki zakres uprawnień do systemów, który jest niezbędny do realizacji zadań im powierzonych,
   c. pracownicy Podmiotu Zewnętrznego mogą uzyskiwać dostęp wyłącznie do standardowych systemów wykorzystywanych w obrębie komórek/ działów, dla których zadania realizują,
   d. w celu zachowania integralności przydzielonych uprawnień z rzeczywistymi potrzebami, wykonywana jest okresowo weryfikacja kont użytkowników,
   e. wszystkie uprawnienia związane z dostępem elektronicznym oraz fizycznym zostają bezwzględnie odebrane w przypadku rozwiązania umowy z Pomiotem Zewnętrznym lub w przypadku odejścia jego pracownika. Podmiot Zewnętrzny zobligowany jest do poinformowania w tym zakresie niezwłocznie pisemnie Kierownika Działu Zarządzania i Informatyzacji.
10) Instalacja aplikacji – obowiązuje zakaz instalacji aplikacji na sprzęcie należącym do Centrum bez zgody Administratora Systemów.
11) Incydenty bezpieczeństwa i naruszenia ochrony danych – pracownicy Podmiotu Zewnętrznego zobowiązani są do pisemnego zgłaszania Inspektorowi Ochrony Danych (iod@co.bydgoszcz.pl, tel. 52 374 3730) incydentów bezpieczeństwa, które mają związek z zadaniami realizowanymi na rzecz Centrum. Pracownicy Podmiotu Zewnętrznego zobowiązani są do przekazania Inspektorowi Ochrony Danych w terminie z nim ustalonym harmonogramu wdrożenia działań naprawczych w odniesieniu do zidentyfikowanego incydentu.
12) Zwrot aktywów – Podmiot Zewnętrzny zobowiązany jest do zwrotu wszystkich aktywów powierzonych na Centrum na czas realizacji zadania/usługi.
13) Audyt drugiej strony - w celu zapewnienia bezpieczeństwa informacji należących do Centrum i przetwarzanych przez Pomiot Zewnętrzny, Centrum zastrzega sobie możliwość wykonania audytu przez pracowników Centrum lub firmę zewnętrzną.

.....
(data i podpis składającego oświadczenie)