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 z klasyfikacji informacji i sposobu jej zabezpieczania oraz poddawane są cyklicznym szkoleniom z zakresu 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 zestawionego między sprzętem pracownika Podmiotu Zewnętrznego a zasobami Centrum tunelu 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 pracownikowi Podmiotu Zewnętrznego na jego wniosek i jest powiązany z jego telefonem służbowym oraz z adresem mailowym w domenie Podmiotu Zewnętrznego,
    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) wszelkie wykryte podatności muszą być niezwłocznie zgłoszone Pełnomocnikowi ds. cyberbezpieczeństwa w Dziale Zarządzania i Informatyzacji Centrum *mailowo na adres cyber@co.bydgoszcz.pl*;
    f) zabronione jest wykorzystywanie podatności zidentyfikowanych przez osoby korzystające z infrastruktury IT Centrum,
    g) osoby korzystające ze zdalnego dostępu muszą zapewnić, że zdalny komputer posiada zainstalowane aktualne oprogramowanie chroniące przed złośliwym kodem,

Podstawowe wymagania dotyczące bezpieczeństwa informacji dla Podmiotów Zewnętrznych

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.

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 *„minimalny"* zakres uprawnień do systemów, który jest niezbędny do realizacji zadań im powierzonych,

c) pracownicy Podmiotu Zewnętrznego mogą uzyskiwać dostęp wyłącznie do urządzeń i systemów, którymi administrują,

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. W tym przypadku Podmiot Zewnętrzny zobligowany jest do poinformowania w tym zakresie niezwłocznie pisemnie Kierownika Działu Zarządzania i Informatyzacji *lub mailowo dzi@co.bydgoszcz.pl.*

10) Instalacja aplikacji – *pracownicy Podmiotu Zewnętrznego odpowiedzialni za instalację oprogramowania na sprzęcie Centrum zobowiązani są do przestrzegania poniższych zasad:*

a) w celu uniknięcia potencjalnych konfliktów z istniejącym oprogramowaniem, zapewnienie zgodności z polityką bezpieczeństwa Centrum, zapewnienie najmniejszej uciążliwości dla działania Centrum, przed instalacją nowego oprogramowania, pracownicy Podmiotu Zewnętrznego powinni zgłaszać tą informację mailowo na adres: dzi@co.bydgoszcz.pl, do oceny i zatwierdzenia przez Administratora Systemów oraz dokładnie określić cel instalacji, rodzaj instalowanego oprogramowania, zakres dostępu danej aplikacji do zasobów Centrum ewentualne zmiany wprowadzone do systemu,

b) każda instalacja powinna być zgodna z zasadami minimalnego uprzywilejowania,

c) pracownicy Podmiotu Zewnętrznego zobowiązani są do aktualizacji oprogramowania systemowego, narzędziowego i użytkowego, w tym zabezpieczeń, aby zapewnić bieżące i skuteczne wsparcie dla infrastruktury Centrum,

d) zakazane jest wyłączanie zabezpieczeń informatycznych. Jeśli istnieje potrzeba tymczasowego wyłączenia zabezpieczeń na czas serwisowy, należy to zgłosić na adres

Podstawowe wymagania dotyczące bezpieczeństwa informacji dla Podmiotów Zewnętrznych

mailowy: cyber@co.bydgoszcz.pl, określając cel, rodzaj prac serwisowych, termin oraz czas na jaki zabezpieczenie ma być zatrzymane,

e) *zabrania się instalacji i uruchamiania oprogramowania, które omija zabezpieczenia lub obniża poziom bezpieczeństwa informatycznego Centrum,*

f) *obowiązuje zakaz instalacji i uruchamiania oprogramowania umożliwiającego dostęp zdalny do zasobów sprzętowych i programowych z sieci publicznych, inny niż wymieniony w pkt 7 na sprzęcie należącym do Centrum bez zgody Administratora Systemów,*

g) *pracownicy Podmiotu Zewnętrznego są odpowiedzialni za upewnienie się, że instalowane oprogramowanie posiada odpowiednie licencje i jest legalnie nabywane, zgodnie z obowiązującymi przepisami prawa. Niedopuszczalna jest instalacja i uruchamianie oprogramowania nielicencjonowanego lub niezgodnego z warunkami licencji.*

11) *Autoryzacja użytkownika – pracownicy Podmiotu Zewnętrznego logujący się do zasobów Centrum zobowiązani są do przestrzegania poniższych zasad:*

a) *każdy zdefiniowany użytkownik oraz administrator systemu zobowiązany jest korzystać z indywidualnego konta, zabezpieczonego unikalnym hasłem,*

b) *gdy to możliwe, należy włączyć i skonfigurować uwierzytelnianie wieloskładnikowe w celu podniesienia poziomu bezpieczeństwa informatycznego,*

c) *wszystkie używane hasła powinny być unikalne, poufne, mieć przynajmniej 12 znaków i zawierać kombinację dużych, małych liter, cyfr oraz znaków specjalnych,*

d) *"1 konto - 1 hasło" nakłada na użytkownika obowiązek posiadania unikalnego hasła dla każdego konta, jednocześnie eliminując używanie tego samego hasła w kilku systemach, zarówno w Centrum, jak i poza nim,*

e) *hasła administracyjne powinny być zmieniane co najmniej co pół roku. W przypadku wdrożonego uwierzytelniania wieloskładnikowego, zmiana hasła dla danego konta powinna odbywać się przynajmniej raz do roku,*

f) *w sytuacji skompromitowania hasła, administratorzy systemu zobowiązani są do niezwłocznej zmiany skompromitowanego hasła zgodnego z ww zasadami lub jeśli to niemożliwe tymczasowej dezaktywacji/blokady konta.*

12) Incydenty bezpieczeństwa i naruszenia ochrony danych osobowych – pracownicy Podmiotu Zewnętrznego zobowiązani są do *niezwłocznego* pisemnego lub telefonicznego zgłaszania:

a) *Inspektorowi Ochrony Danych (iod@co.bydgoszcz.pl, tel. 52 374 3730) naruszeń ochrony danych osobowych, 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.*

b) *Pełnomocnikowi ds. Cyberbezpieczeństwa (cyber@co.bydgoszcz.pl, tel. 52 374 3947) incydentów z zakresu bezpieczeństwa informatycznego, które zostały zidentyfikowane przez Pracowników Podmiotu Zewnętrznego, podczas realizacji zadań na rzecz Centrum*

13) Zwrot aktywów - Podmiot Zewnętrzny zobowiązany jest do zwrotu wszystkich aktywów powierzonych na Centrum na czas realizacji zadania/usługi.

14) Audyt drugiej strony - w celu zapewnienia *wysokiego poziomu* bezpieczeństwa informacji należących do Centrum i przetwarzanych przez Pomiot Zewnętrzny, Centrum zastrzega sobie możliwość wykonania audytu przez pracowników Centrum lub firmę zewnętrzną.

Podstawowe wymagania dotyczące bezpieczeństwa informacji dla Podmiotów Zewnętrznych

15) Monitorowanie – *w celu zapewnienia wysokiego poziomu bezpieczeństwa informatycznego i zasobów cyfrowych, Centrum zastrzega sobie możliwość:*

a) *monitorowania zgodności używanych haseł z polityką bezpieczeństwa informacji,*
b) *monitorowanie nieudanych prób logowania i zawieszania kont w przypadku stwierdzenia naruszenia polityki bezpieczeństwa informacji,*
c) *nagrywania działań administratora podczas sesji połączenia zdalnego z zasobami Centrum,*
d) *weryfikacji poziomu bezpieczeństwa konfiguracji i poziomu podatności oprogramowania zainstalowanego przez Podmiot Zewnętrzny w zasobach Centrum. W sytuacji stwierdzenia błędnej konfiguracji, konfiguracji obniżającej poziom bezpieczeństwa informatycznego lub ujawnienia krytycznej podatności zainstalowanego oprogramowania, Podmiot Zewnętrzny powinien niezwłocznie, w terminie narzuconym przez Centrum, dokonać zmian konfiguracyjnych lub usunięcia luki w zabezpieczeniach informatycznych. Ewentualne wydłużenie tego terminu może nastąpić wyłącznie za zgodą Centrum, na pisemny wniosek na adres email: cyber@co.bydgoszcz.pl,*
e) *podjęcie własnych środków bezpieczeństwa, w celu ochrony zasobów informatycznych Centrum w postaci wyłączenia niektórych usług np. odłączenia możliwości wykonywania zdalnego połączenia*

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

Adresy e-mail do kontaktu:
1. *iod@co.bydgoszcz.pl – Inspektor Ochrony Danych*
2. *cyber@co.bydgoszcz.pl – Pełnomocnik ds. Cyberbezpieczeństwa*
3. *dzi@co.bydgoszcz.pl – Dział Zarządzania i Informatyzacji*