POLITYKA BEZPIECZEŃSTWA INFORMACJI DLA WYKONAWCÓW CENTRUM E-ZDROWIA

ZINTEGROWANY SYSTEM ZARZĄDZANIA

ZSZ.SZBI.ISO.P.A.15

METRYKA DOKUMENTU

Opis	Dokument opisuje zasady bezpieczeństwa informacji w relacjach z Wykonawcami Centrum		
Nazwa pliku	ZSZ.SZBI.ISO.P.A.15._Polityka-Bezpieczenstwa-Informacji-dla-wykonawcow_IP_v.1.2		
Właściciel	dyrektor Centrum e-Zdrowia		
Autorzy	Piotr Rybicki, Piotr Kuśmierski, Kamila Stęplowska, Kamil Bugnacki		
Zatwierdzający	dyrektor DB		
Sygnatura wg ISO 27001:2017	ZSZ.SZBI.ISO.P.A.15		
Sygnatura wg ISO 27001:2022	ZSZ.SZBI.ISO.P.A.5.19		
Wersja dokumentu	1.2	**Status**	Zatwierdzony
Data zatwierdzenia	2024-05-15	**Klasyfikacja**	Do użytku publicznego
Obowiązuje od	2024-05-22	**Wycofano dnia**	-

ROZDZIELNIK DOKUMENTU

Aktualna wersja niniejszego dokumentu w wersji elektronicznej, dostępna jest w intranecie CeZnet-> Pigułka wiedzy -> Zintegrowany System Zarządzania
Link do strony: (https://csioz.sharepoint.com/portal_bezpieczenstwo/)
Dokumenty w wersji papierowej są wyłącznie materiałami informacyjnymi.

HISTORIA ZMIAN

WERSJA	DATA	ROZDZIAŁ	OPIS ZMIAN	IMIĘ I NAZWISKO
0.1	2021-04-14	-	Utworzenie dokumentu	-
1.0	2021-06-30	-	Akceptacja dokumentu bazowego	-
1.1	2023-03-22	4.1, 4.3, załącznik	4.1 - Zaktualizowano zapisy dotyczące danych osobowych 4.3 - Zaktualizowano długość i liczbę pamiętanych haseł Wydzielono załącznik do osobnego dokumentu.	Rybicki Piotr z zespołem: Kamila Stęplowska, Piotr Kuśmierski, Kamil Bugnacki
1.2	2024-05-14	3 4 5.1	Dodano pkt 4 i 5 dot. konfliktu interesów Dodano rozdział 4 referujący do Polityki ochrony fizycznej. Zaktualizowano zapisy pkt 4a i 4b.	Rybicki Piotr z zespołem: Kamila Stęplowska, Piotr Kuśmierski, Kamil Bugnacki, Michał Skoczylas

PRZEGLĄDY DOKUMENTU

LP.	DATA PRZEGLĄDU		PRZEGLĄDU DOKONAŁ (nazwisko i imię)	ADNOTACJE
	BIEŻĄCEGO	NASTĘPNEGO		
1	2023-03-22	2024-03-22	Rybicki Piotr z zespołem: Kamila Stęplowska, Piotr Kuśmierski, Kamil Bugnacki	Przegląd, modyfikacja dokumentu oraz dostosowanie szaty graficznej.

SPIS TREŚCI

1. Definicje i skróty

Terminy i skróty użyte w niniejszym dokumencie zostały wyjaśnione w dokumencie: ZSZ.SZBI.ISO_Slownik-definicji-i-skrotow.

2. Wprowadzenie

2.1. Cel polityki

Celem Polityki Bezpieczeństwa Informacji dla Wykonawców zwanej dalej Polityką jest zapewnienie bezpieczeństwa systemów budowanych, rozwijanych i eksploatowanych przez Wykonawców Centrum, a także bezpieczeństwa realizacji zadań na rzecz Centrum, poprzez m.in. określenie minimalnych wymagań w zakresie bezpieczeństwa informacji oraz zabezpieczeń systemów teleinformatycznych.

2.2. Zakres stosowania

Niniejsza Polityka obowiązuje wszystkich Wykonawców Centrum uzyskujących dostęp, przetwarzających, przechowujących, przesyłających lub dostarczających elementy infrastruktury teleinformatycznej dla przetwarzania informacji należących do Centrum. Niniejszy dokument dotyczy wszystkich systemów informatycznych, które są wdrażane, rozwijane bądź utrzymywane, będących własnością Centrum, lub powierzonych do utrzymania.

Postanowienia niniejszej Polityki należy stosować we wszystkich umowach z Wykonawcami, których przedmiot jest związany z ochroną informacji.

2.3. Przeglądy i aktualizacja

Polityka i zawarte w niej informacje są poddawane przeglądowi w cyklu rocznym, począwszy od daty jej wdrożenia, a w sytuacji stwierdzenia rozbieżności bezzwłocznie. Celem przeglądu jest weryfikacja czy polityka skutecznie realizuje strategię Centrum. Za przegląd i aktualizację niniejszego dokumentu odpowiedzialny jest Pełnomocnik ds. ZSZ.

2.4. Wyłączenia

Z niniejszej Polityki wyłączone są informacje niejawne oraz dedykowane systemy przetwarzania informacji niejawnych dla których stosowane są odrębne przepisy[1].

[1] Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz.U. z 2023 r. poz. 756 z późniejszymi zmianami).

3. Postanowienia ogólne

1. Niniejsza Polityka określa zakres obowiązków i odpowiedzialności Wykonawców w zakresie bezpieczeństwa informacji. Obejmuje swym zakresem wszystkich Wykonawców, mających dostęp do systemów informacyjnych Centrum. Polityka jest syntezą informacji zawartych w Polityce Bezpieczeństwa Informacji Centrum e-Zdrowia.
2. Wykonawca musi spełniać wymagania niniejszej Polityki przed uzyskaniem dostępu do infrastruktury i systemów teleinformatycznych Centrum.
3. Przed rozpoczęciem przetwarzania informacji chronionych, w szczególności danych osobowych, Wykonawca musi spełniać warunki:
   a) przeszkolić pracowników i osoby trzecie realizujące w jego imieniu zadania na rzecz Centrum, w zakresie zachowania zasad bezpieczeństwa informacji i podpisać zobowiązanie do zachowania poufności przetwarzanych danych, będących załącznikiem do Umowy,
   b) każda osoba, która w imieniu Wykonawcy bezpośrednio uczestniczy w realizacji przedmiotu Umowy na rzecz Centrum zobowiązana jest do zapoznania się z niniejszą Polityką i podpisania przed przystąpieniem do realizacji zadań, imiennego oświadczenia, którego wzór stanowi załącznik ZSZ.SZBI.ISO.P.A.15.Z.1._Oswiadczenie-o- zapoznaniu-sie-z-Polityka-Bezpieczenstwa-Informacji-dla-Wykonawcow.docx do niniejszej Polityki,
   c) w przypadku powierzenia przetwarzania danych osobowych Centrum, podpisać umowę powierzenia przetwarzania danych osobowych zgodnie ze wzorem obowiązującym w Centrum.
4. Wykonawca winien zapewniać przez cały okres współpracy z Centrum, że nie występuje konflikt interesów w stosunku do niego, członków jego władz oraz w stosunku do jakichkolwiek osób lub podmiotów uczestniczących ze strony Wykonawcy w realizacji umowy z Centrum, w szczególności personelu lub Podwykonawców oraz zobowiązuje się do niepodejmowania jakichkolwiek działań, które mogą prowadzić do powstania konfliktu interesów. Przez konflikt interesów Zamawiający rozumie istnienie okoliczności, które mają lub mogłyby mieć wpływ na rzetelność, bezstronność i obiektywność przy realizacji umowy z Centrum. W przypadku wystąpienia lub możliwości wystąpienia potencjalnego konfliktu interesów, Wykonawca jest zobowiązany do pisemnego lub w formie elektronicznej poinformowania Zamawiającego o konflikcie interesów wraz z udzieleniem niezbędnych wyjaśnień oraz jego usunięcia lub zapobieżenia mu.
5. Od udziału w wykonaniu umowy wyłączony jest personel Wykonawcy lub podwykonawcy, w stosunku do których występuje konflikt interesów. W ramach współpracy z Centrum nie może dochodzić do łączenia ról lub funkcji, które prowadziłyby do konfliktu interesów lub negatywnie wpływałoby na zabezpieczenie interesów Centrum.

4. Zasady poruszania się Wykonawców w siedzibie Centrum

1. Pracownikom Wykonawców wydawane są karty “Gość”. Zasady wydawania i poruszania się po Centrum opisane są w Procedurze ochrony fizycznej obiektu (ZSZ.SZBI.ISO.PR.A.11.1).
2. Firmy mające stałe umowy i świadczące usługi w siedzibie Centrum są zobowiązane do zapoznania swoich pracowników z zasadami obowiązującymi w CeZ na podstawie Polityki ochrony fizycznej obiektu (ZSZ.SZBI.ISO.P.A.11).
3. Powyższe punkty stosuje się w przypadku, gdy pracownik Wykonawcy musi przebywać na terenie Centrum.

5. Dostęp do środowiska teleinformatycznego Centrum

1. Wykonawca zobowiązany jest wykorzystywać przyznany dostęp wyłącznie w celach i w zakresie uzasadnionym realizacją zadań wynikających z przedmiotu Umowy, zgodnie z Umową oraz obowiązującymi przepisami prawa.
2. Wykonawca zobowiązany jest zapewnić właściwą ochronę udostępnionych mu systemów lub zasobów informacyjnych Centrum, polegającą w szczególności na zapewnieniu zespołu środków organizacyjnych, technicznych i prawnych stosowanych w celu zapewnienia bezpieczeństwa informacji.
3. Dostęp do krytycznych zasobów Centrum realizowany jest wyłącznie z użyciem stacji przesiadkowych udostępnianych przez Centrum. Sesje takie są izolowane, monitorowane i nagrywane w czasie rzeczywistym.
4. W związku z dostępem do środowiska teleinformatycznego Centrum, Wykonawca ma obowiązek stosować się do zaleceń oraz wymagań Centrum mających na celu zapewnienie bezpieczeństwa informacji, w tym m.in. zapoznać własny personel i zapewnić przestrzeganie wskazanych przez Centrum zasad bezpiecznego użytkowania systemu teleinformatycznego oraz zasad bezpiecznego użytkowania środowiska biurowego. Wykonawca jednocześnie zapewnia, że dostęp do systemów lub zasobów teleinformatycznych Centrum będą posiadać wyłącznie uprawnieni i przeszkoleni pracownicy/współpracownicy, w zakresie i na czas niezbędny do realizacji przez nich przedmiotu Umowy.
5. Za sprawowanie nadzoru nad korzystaniem przez Wykonawcę z dostępu do systemów lub zasobów teleinformatycznych odpowiedzialna jest Opiekun Osoby Trzeciej.
6. Bez uszczerbku dla postanowień Umowy, Wykonawca ponosi pełną odpowiedzialność za działania swoich pracowników/współpracowników w systemach lub zasobach teleinformatycznych Centrum oraz za wszelkie szkody powstałe w związku z korzystaniem przez Wykonawcę z dostępu do systemów lub zasobów teleinformatycznych Centrum w sposób sprzeczny z niniejszą Polityką.
7. Bez uszczerbku dla postanowień Umowy, w sytuacji korzystania przez Wykonawcę przy realizacji Umowy z usług podwykonawców, Wykonawca zapewnia przestrzeganie przez te podmioty oraz osoby realizujące w ich imieniu Umowę wszystkich wymagań bezpieczeństwa Centrum, o których mowa w niniejszej Polityce i ponosi w tym zakresie pełną odpowiedzialność względem Centrum.
8. Brak dostępu do systemów lub zasobów teleinformatycznych Centrum po stronie Wykonawcy, nie może być podstawą do dochodzenia od Centrum jakichkolwiek roszczeń.

5.1. Nadawanie, modyfikacja i wycofanie uprawnień

1. Dostęp Wykonawcy do środowiska teleinformatycznego Centrum odbywa się wyłącznie na zasadach określonych w niniejszej Polityce.
2. Uprawnienia, przyznaje się Wykonawcy jedynie na czas określony, nie dłuższy niż 12 miesięcy i w zakresie niezbędnym do właściwego wykonywania przedmiotu Umowy. Po upływie tego czasu, przedłużenie dostępu Dostawcy do systemów lub zasobów teleinformatycznych Centrum może nastąpić wyłącznie po ponownej weryfikacji zakresu oraz warunków jego przyznania, z zachowaniem procedur, o których mowa w niniejszej Polityce.
3. Dostęp może być udzielony wyłącznie osobom, które zostały jednoznacznie zidentyfikowane przez Opiekuna Osoby Trzeciej i którym na zasadach obowiązujących w Centrum, przydzielono Tożsamość Cyfrową.

4. Stworzenie Tożsamości Cyfrowej wymaga podania:
   a) imienia i nazwiska, numeru PESEL oraz daty urodzenia - w przypadku obywatela polskiego lub osób odpowiedzialnych za bezpieczeństwo systemów teleinformatycznych w Centrum niezależnie od podstawy zatrudnienia;
   b) imienia i nazwiska, daty urodzenia, rodzaju, serii i numeru dokumentu tożsamości – w przypadku osoby nie posiadającej obywatelstwa polskiego i nieposiadającego numeru PESEL, z zastrzeżeniem lit a).
5. Lista Użytkowników ze strony Wykonawcy, powinna być dostarczona przez osoby wskazane w Umowie, jako odpowiedzialne za jej realizację. Po każdej zmianie Użytkowników ze strony Wykonawcy, jest on zobowiązany do przekazania listy Użytkowników ze wskazaniem zmian w zakresie ich uprawnień.
   a) Nadawanie, zmiana, bądź wycofanie uprawnień jest realizowane przez pracowników Centrum, zgodnie z poniższym schematem postępowania:
   b) Opiekun Osoby Trzeciej, występuje o przydzielenie Tożsamości Cyfrowej dla Użytkowników będących personelem Wykonawcy, zgodnie z procedurami obowiązującymi w Centrum.
   c) Na podstawie postanowień Umowy z Wykonawcą, Opiekun Osoby Trzeciej ustala niezbędny zakres uprawnień dla poszczególnych Użytkowników będących personelem Wykonawcy.
   d) Opiekun Osoby Trzeciej występuje o nadanie, zmianę lub wycofanie uprawnień do systemu informatycznego, zgodnie z polityką (ZSZ.ISO.P.01_Polityka-Dostepu-do-Srodowiska-Teleinformatycznego).
   e) Administrator IT Centrum nadaje, modyfikuje bądź wycofuje uprawnienia zgodnie ze złożonym wnioskiem. W przypadku rejestracji nowego Użytkownika, nadawany jest unikalny identyfikator oraz ustawiane jest Hasło Tymczasowe, niezbędne do pierwszego logowania w Systemie.
   f) Po nadaniu, zmianie lub wycofaniu uprawnień w określonych systemach informatycznych, Administrator IT informuje o tym zdarzeniu Wykonawcę za pośrednictwem Opiekuna Osoby Trzeciej.
6. W przypadku zakończenia przez Wykonawcę współpracy z pracownikiem /współpracownikiem, Wykonawca bezzwłocznie informuje Opiekuna Osoby Trzeciej o zmianach personalnych. Brak zgłoszenia zakończenia współpracy przenosi wszelką odpowiedzialność za aktywność danego Użytkownika na Wykonawcę.

5.2. Odebranie dostępu

1. Dostęp do środowiska teleinformatycznego Centrum dla Wykonawcy jest odbierany niezwłocznie w następujących przypadkach:
   a) z upływem czasu, na który dostęp został przyznany;
   b) jeśli dalszy dostęp do środowiska teleinformatycznego nie jest niezbędny Wykonawcy do realizacji umowy;
   c) w wyniku decyzji Inspektora Ochrony Danych o zablokowaniu Wykonawcy lub pracownikowi/współpracownikowi Wykonawcy, ze skutkiem natychmiastowym, przyznanego dostępu w przypadku, gdy dalszy dostęp zagraża bezpieczeństwu danych osobowych będących własnością, bądź powierzonych Centrum;
   d) w wyniku decyzji Dyrektora Departamentu Bezpieczeństwa lub osoby przez niego upoważnionej o zablokowaniu Wykonawcy lub pracownikowi/współpracownikowi Wykonawcy, ze skutkiem natychmiastowym, przyznanego dostępu:

- w przypadku, gdy dalszy dostęp Wykonawcy lub pracownikowi/współpracownikowi Wykonawcy do systemów lub zasobów teleinformatycznych Centrum zagraża bezpieczeństwu informacji lub;
- w przypadku stwierdzenia rażącego naruszenia przez Wykonawcę lub pracownika/współpracownika Wykonawcy postanowień niniejszej Polityki.

5.3. Metody i środki uwierzytelniania

1. Metody i środki uwierzytelniania opisane zostały w ZSZ.ISO.P.01._Polityka-Dostepu-do-Srodowiska-Teleinformatycznego
2. Dostęp do środowiska teleinformatycznego Centrum może mieć wyłącznie Użytkownik po podaniu identyfikatora (loginu) i właściwego hasła.
3. Hasła Użytkowników podlegają zasadom zgodnie z polityką haseł (pkt 8 ZSZ.ISO.P.01-Polityka_Dostepu_do_Srodowiska_Teleinformatycznego)

6. Minimalne wymagania bezpieczeństwa

1. Wykonawca musi zapewnić, że zadania realizowane na rzecz Centrum będą zarządzane zgodnie z najlepszymi praktykami określonymi w normie PN-ISO/IEC 27002 w rozdziale pt. „Bezpieczeństwo Informacji w zarządzaniu projektami” (6.1.5) oraz wymaganiami niniejszej Polityki. W szczególności musi zostać zapewnione, aby:
   a) zidentyfikował cele bezpieczeństwa realizowanego przedsięwzięcia,
   b) zidentyfikował i oszacował ryzyka związane z realizacją przedsięwzięcia,
   c) zdefiniował i zastosował zabezpieczenia adekwatne do zidentyfikowanych ryzyk,
   d) opracował plany ciągłości gwarantujący bezpieczeństwo usług świadczonych dla Centrum.
2. Wykonawca winien stosować klasyfikację informacji przesyłanej, przechowywanej i przetwarzanej w kontekście realizacji zadań na rzecz Centrum, zgodnie z zasadami klasyfikacji opisanymi w niniejszym dokumencie oraz najlepszymi praktykami określonymi w normie PN-ISO/IEC 27002 w rozdziale pt. „Klasyfikacja Informacji” (8.2).
3. Wykonawca jest zobowiązany do zapewnienia, przy dochowaniu najwyższej staranności, właściwej ochrony udostępnionego środowiska teleinformatycznego Centrum, w szczególności wdrożenia po swej stronie mechanizmów organizacyjno-technicznych gwarantujących:
   a) dostęp do systemów lub zasobów teleinformatycznych wyłącznie dla uprawnionych Użytkowników,
   b) rozliczalność Użytkowników, rozumianą jako możliwość jednoznacznego przypisania działań prowadzonych w systemie lub zasobie do konkretnego Użytkownika.
4. Realizując wymagania, o których mowa w pkt. 2, Wykonawca zapewni w szczególności:
   a) ochronę wszelkich udostępnionych mu przez Centrum urządzeń, a także wszystkich komponentów sprzętowych (np. klucze kryptograficzne), kart dostępu fizycznego oraz programowych (np. dedykowanej aplikacji) oraz wszelkich informacji (np. loginy i hasła) przed dostępem osób nieuprawnionych,
   b) skuteczne mechanizmy organizacyjne i techniczne uniemożliwiające Użytkownikom:
      - dokonywanie prób sprawdzania, testowania i omijania zabezpieczeń systemów teleinformatycznych Centrum,
      - podejmowanie działań, które pośrednio lub bezpośrednio mogą prowadzić do naruszenia bezpieczeństwa udostępnionych systemów lub zasobów teleinformatycznych.

5. Wykonawca musi zapewnić bezpieczeństwo informacji przesyłanej w związku z realizacją zadań na rzecz Centrum zgodnie wymaganiami określonymi w rozdziale normy PN-ISO/IEC 27002 pt. „Przesyłanie informacji” (13.2). W szczególności musi:
   a) zapewnić ochronę poufności oraz integralności informacji przesyłanej publicznymi kanałami transmisyjnymi, odpowiednio do jej klasy bezpieczeństwa,
   b) zapewnić, że wszystkie osoby mające dostęp do informacji chronionych lub szczególnie chronionych podpisały klauzule poufności,
   c) zapewnić szyfrowanie komunikacji w oparciu o rozwiązania zapewniające poziom bezpieczeństwa, co najmniej równy temu jaki zapewniają protokoły TLS w wersji co najmniej 1.2 lub VPN.
6. Wykonawca musi zidentyfikować i udokumentować łańcuch dostaw związany z realizacją Umowy. Musi zapewnić, że jego podwykonawcy zapewniają taki sam poziom bezpieczeństwa jaki spełnia on sam w odniesieniu do Centrum. Wykonawca odpowiada za zapewnienie bezpieczeństwa w całym łańcuchu dostaw produktów i usług, za który jest odpowiedzialny zgodnie z zawartą Umową. Wytyczne do realizacji tego wymagania określają najlepsze praktyki zawarte w rozdziałach normy PN-ISO/IEC 27002 pt. „Prace rozwojowe zlecane podmiotom zewnętrznym” (14.2.7) i „Łańcuch dostaw technologii informacyjnych i teleinformacyjnych” (15.1.3).
7. Wykonawca winien zapewnić bezpieczeństwo wykorzystywanego personelu zgodnie z najlepszymi praktykami określonymi w rozdziałach norm PN-ISO/IEC 27002 pt. „Odpowiedzialność kierownictwa” (7.2.1), „Uświadamianie, kształcenie i szkolenia z zakresu bezpieczeństwa informacji” (7.2.2) oraz „Zakończenie zatrudnienia lub zmiana zakresu obowiązków” (7.3.1), adekwatnie do zadań realizowanych na rzecz Centrum. W szczególności, musi posiadać I realizować udokumentowane polityki dotyczące jego personelu, które obejmują:
   a) przekazanie własnemu personelowi, realizującemu zadania na rzecz Centrum, informacji o wymaganiach bezpieczeństwa współpracy z Centrum,
   b) wdrożenie programu cyklicznych szkoleń z zakresu bezpieczeństwa informacji i cyberbezpieczeństwa, a następnie zapewnienie udział personelu oddelegowanego do współpracy z Centrum w tych szkoleniach.
8. Wykonawca musi zapewnić właściwe użycie aktywów, powierzonych przez Centrum, wykorzystywanych w pracach na rzecz Centrum zgodnie z najlepszymi praktykami określonymi w rozdziałach normy PN-ISO/IEC 27002 pt. „Akceptowalne użycie aktywów” (8.1.3) i „Zwrot aktywów” (8.1.4). W szczególności wymaganym jest aby:
   a) użytkownicy tych 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.
9. Wykonawca winien zapewnić bezpieczeństwo wymiennych nośników danych wykorzystywanych w związku z realizacją zadań na rzecz Centrum zgodnie z najlepszymi praktykami określonymi w rozdziale normy PN-ISO/IEC 27002 pt. „Postępowanie z nośnikami” (8.3). W szczególności musi:
   a) posiadać i realizować polityki dotyczące bezpiecznego usuwania danych z nośników zawierających dane związane z realizacją zadań na rzecz Centrum, zapewniając skuteczne usuwanie,

b) posiadać i realizować polityki bezpiecznego przekazywania nośników zawierających dane związane z realizacją zadań na rzecz Centrum, zapewniając skuteczną ochronę danych.

10. Wszelkie oprogramowanie wykorzystywane w ramach realizacji przez Wykonawcę przedmiotu Umowy musi być użytkowane z poszanowaniem praw własności intelektualnej, w szczególności zgodnie z ustawą o prawie autorskim i prawach pokrewnych.

7. Bezpieczeństwo infrastruktury

1. Do środowiska teleinformatycznego Centrum mogą być podłączane wyłącznie komputery i urządzenia spełniające minimalne wymagania bezpieczeństwa, w szczególności:
   a) system operacyjny posiada zainstalowane wszystkie dostępne aktualizacje zabezpieczeń,
   b) zainstalowano oprogramowanie szyfrujące zawartość dysków twardych,
   c) system antywirusowy jest zainstalowany w systemie operacyjnym, a jego sygnatury są aktualne,
   d) firewall jest uruchomiony w systemie operacyjnym i posiada właściwą konfigurację, odpowiadającą wykonywanym obowiązkom pracowniczym przez Użytkowników komputera,
   e) zainstalowane na komputerze oprogramowanie pochodzi z zaufanych źródeł,
   f) zainstalowane oprogramowanie uzyskało akceptację Departament Bezpieczeństwa CeZ,
   g) oprogramowanie jest zainstalowane zgodnie z postanowieniami licencji producenta oprogramowania.
2. Zabrania się Wykonawcy samodzielnego dokonywania zmian w konfiguracji i oprogramowaniu urządzeń udostępnionych przez Centrum do realizacji dostępu do środowiska teleinformatycznego Centrum, w tym w szczególności podejmowania jakichkolwiek działań powodujących nieskuteczność zastosowanych środków technicznych służących zapewnienia bezpieczeństwa.
3. Urządzenia Wykonawcy, wykorzystywane przez niego do realizacji dostępu do środowiska teleinformatycznego Centrum nie mogą zagrażać bezpieczeństwu informacji. W szczególności Wykonawca zobowiązany jest do zastosowania odpowiednich zabezpieczeń chroniących przed złośliwym oprogramowaniem.
4. Urządzenia Wykonawcy, o których mowa w ust. 2 muszą być chronione w sposób uniemożliwiający bezpośrednie lub pośrednie pozyskanie przez osoby nieupoważnione dostępu do środowiska teleinformatycznego Centrum. Wykonawca w szczególności ma obowiązek wyeliminować możliwość przejęcia kontroli nad tymi urządzeniami lub ich wykorzystania w trakcie komunikacji.
5. Urządzenia oraz oprogramowanie, z których korzysta Wykonawca nie mogą powodować wykorzystania środowisk teleinformatycznych Centrum (w tym zasobów sieciowych) ponad zakres niezbędny do wykonywania działań niezbędnych do realizacji przedmiotu Umowy oraz wynikających z zakresu przyznanego dostępu oraz powodować niedostępność środowiska.
6. Zabrania się podejmowania prób sprawdzania, testowania i omijania zabezpieczeń systemów informatycznych Centrum, z wyłączeniem zadań realizowanych na mocy Umowy dotyczącej przeprowadzenia autoryzowanych testów bezpieczeństwa.
7. Centrum zastrzega sobie prawo do pełnej kontroli udostępnionych, jak i będących własnością Wykonawcy urządzeń, z których realizowany jest dostęp do środowiska teleinformatycznego Centrum.

8. Stosowanie zabezpieczeń kryptograficznych

1. W celu ochrony poufności przesyłanych oraz przechowywanych danych stosuje się zabezpieczenia kryptograficzne. Zabezpieczenia powinny być zgodne z wymaganiami prawnymi oraz regulacjami wewnętrznymi, w szczególności należy stosować zabezpieczenia kryptograficzne:
   a) na dyskach twardych komputerów przenośnych,
   b) na pamięciach wymiennych typu pendrive, dysk zewnętrzny itp.
   c) na nośnikach kopii zapasowych przechowywanych poza systemem informatycznym Centrum,
   d) tunelach VPN,
   e) korespondencji elektronicznej, w trakcie przesyłania danych objętych ochroną, w szczególności dane osobowe.
2. Zakres stosowanych rozwiązań kryptograficznych powinien obejmować minimum dane znajdujące się na nośnikach, które objęte są ochroną ze względu na wymagania utrzymania odpowiedniego poziomu poufności.
3. Rozwiązania kryptograficzne powinny wykorzystywać algorytm AES (lub mocniejszy) o długości klucza minimum 256 bit.

9. Dostęp zdalny

1. Dostęp zdalny Wykonawców, możliwy jest na zasadach i na czas określony zapisami Umowy i tylko po spełnieniu warunków wymienionych w niniejszej *Polityce*.
2. Wniosek o dostęp zdalny dla przedstawicieli Wykonawcy w zakresie wynikającym z realizowanych zadań, składa Opiekun Osoby Trzeciej zgodnie z wewnętrznymi procedurami.
3. Wykonawca winien zapewnić bezpieczeństwo wykonywania na rzecz Centrum pracy zdalnej oraz wykorzystywanych urządzeń mobilnych zgodnie z najlepszymi praktykami określonymi w rozdziale normy PN-ISO/IEC 27002 pt. „Polityka stosowania urządzeń mobilnych" (6.2.1.). W szczególności musi posiadać i realizować udokumentowaną politykę korzystania z urządzeń mobilnych, która zapewnia:
   a) ochronę fizyczną urządzeń przenośnych (smartphone/tablety/notebooki),
   b) nadzór nad oprogramowaniem instalowanym na urządzeniach mobilnych oraz stosowania uaktualnień,
   c) zarządzanie uprawnieniami dostępu do urządzeń mobilnych,
   d) ochronę urządzeń mobilnych przed szkodliwym oprogramowaniem,
   e) zarządzanie technikami kryptograficznymi, które zapewnią bezpieczeństwo przechowywanych danych,
   f) ograniczenia w połączeniach do usług informacyjnych,
   g) zasady wykonywania kopii bezpieczeństwa,
   h) bezpieczeństwo zdalnego zarządzania urządzeniami.
4. Wykonawca musi zapewnić bezpieczeństwo pracy zdalnej w środowisku teleinformatycznym Centrum, zgodnie z najlepszymi praktykami określonymi w rozdziale normy pt. „Telepraca" (6.2.2). W szczególności:
   a) dostęp do zasobów Centrum musi być realizowany wyłącznie z wykorzystaniem środowiska teleinformatycznego i informacji udostępnionych przez Centrum,
   b) dostęp do zasobów Centrum musi być wykorzystywany tylko w celach i zakresie określonym przez Centrum,

c) przedstawiciele Wykonawcy posługują się wyłącznie indywidualnym loginem służącym do identyfikacji w systemach informatycznych Centrum; zabronione jest współdzielenie loginów i haseł,
d) Użytkownicy ze strony Wykonawcy, korzystający ze zdalnego dostępu zobowiązani są do zapewnienia ochrony fizycznej zasobów oraz zachowania poufności informacji niezbędnych do korzystania ze zdalnego dostępu,
e) wykorzystanie zdalnego dostępu musi być realizowane warunkach, które będą zabezpieczały przed ujawnieniem informacji poufnych,
f) zabronione jest testowanie i wykorzystywanie podatności w zdalnym dostępie zidentyfikowanych przez osoby korzystające ze zdalnego dostępu,
g) wszelkie wykryte podatności muszą być niezwłocznie zgłoszone do Departamentu Bezpieczeństwa Centrum bezpośrednio, bądź poprzez Opiekuna Strony Trzeciej. Dalsze korzystanie ze zdalnego dostępu winno być realizowane wyłącznie po wyrażeniu zgody przez Departament Bezpieczeństwa Centrum,
h) osoby korzystające ze zdalnego dostępu muszą zapewnić, że zdalny komputer nie jest jednocześnie podłączony do innej sieci komputerowej, ewentualnie za wyjątkiem sieci komputerowej Centrum,
i) osoby korzystające ze zdalnego dostępu muszą zapewnić, że zdalny komputer posiada zainstalowane aktualne oprogramowanie chroniące przez złośliwym kodem, które posiada aktualizowaną bazę sygnatur,
j) Departament Bezpieczeństwa Centrum ma prawo do ciągłego monitorowania wszelkiej aktywności sieciowej w systemach należących do Centrum,
k) Centrum ma prawo do rejestrowania, przechowywania i wykorzystania w celach dowodowych wszelkich zdarzeń związanych z realizacją zdalnego dostępu.

5. Zabrania się dostępu zdalnego z publicznych otwartych sieci WiFi.
6. Zabrania się dostępu zdalnego z komputerów dostępnych publicznie (nie zarządzanych przez Centrum, bądź Wykonawcę), np. kawiarnie internetowe, dworce i lotniska itp.

10. Bezpieczeństwo środowisk produkcyjnych Centrum

1. W ramach dostępu zabrania się Wykonawcy trwale usuwać dane, przeprowadzać jakiekolwiek operacje na dyskach mogące prowadzić do ich uszkodzenia lub utraty danych, w szczególności ich formatowania.
2. Dla środowisk produkcyjnych (oddanych do eksploatacji) Wykonawca, przed przystąpieniem do prac, przedstawia scenariusz planowanych prac wraz z oceną ryzyka podejmowanych czynności. Wykonawca odpowiada za odstępstwa od przedstawionego scenariusza. Scenariusz powinien obejmować:
   a) kto będzie prowadził prace,
   b) kiedy, przewidywany czas trwania,
   c) zakres wykonywanych prac,
   d) informację czy wymagana jest przerwa w pracy Użytkowników,
   e) potencjalne ryzyka podejmowanych czynności.
3. Przedstawiciel Wykonawcy wykonujący prace, przystępując do czynności, o których wie, że w konsekwencji doprowadzić one mogą do zniszczenia danych, musi poinformować pracownika Centrum odpowiedzialnego za utrzymanie tego Systemu i dopiero po jego pisemnej akceptacji może podjąć te czynności.

4. Wykonywanie prac polegających na standardowej obsłudze serwisowej, prac nad rozwojem programu będącego w fazie wdrażania nie wymaga każdorazowego ustalenia warunków realizacji czynności, będącej ich częścią. W ramach wykonywania tych czynności obowiązują warunki uzgodnione wcześniej. W szczególności nie wymagają każdorazowego ustalenia warunków realizacji te czynności, które wynikają z przedmiotu Umowy i nie są objęte ryzykami opisanymi w pkt. 1. Wykonywanie czynności niestandardowych wymaga każdorazowo określenia warunków.

11. Bezpieczeństwo prac projektowych Wykonawcy

1. Wykonawca winien wykorzystywać w pracach projektowych, realizowanych na rzecz Centrum, najlepsze praktyki określone w rozdziałach normy PN-ISO/IEC 27002 pt. „Polityka bezpieczeństwa prac rozwojowych" (14.2.1), „Procedury kontroli i zmian w systemach", (14.2.2), „Zasady projektowania bezpiecznych systemów" (14.2.5). W szczególności musi:
   a) zapewnić istnienie i realizację udokumentowanych punktów kontrolnych realizacji wymagań bezpieczeństwa,
   b) zapewnić kontrolę wersji wytwarzanego kodu oraz dokumentacji,
   c) zapewnić spełnienie udokumentowanych standardów programowania, przekazanych w ramach realizacji prac,
   d) zapewnić realizację udokumentowanych procedur zarządzania zmianami w wytwarzanych aplikacjach, systemach.
2. Wykonawca winien zapewnić, że zmiany wprowadzane do projektowanych rozwiązań będą realizowane zgodnie z najlepszymi praktykami określonymi w rozdziale normy PN-ISO/IEC 27002 pt. „Zarządzanie zmianami w usługach świadczonych przez dostawców" (15.2.2). W szczególności musi zapewnić, że:
   a) zmiany będą rejestrowane,
   b) zmiany będą zatwierdzane przez upoważnione osoby,
   c) będą istniały procedury zarządzania zmianami w wytwarzanych aplikacjach i systemach.
3. Wykonawca winien zapewnić ochronę dokumentacji projektowej oraz eksploatacyjnej, tworzonej i przetwarzanej na rzecz Centrum, zgodnie z najlepszymi praktykami określonymi w rozdziale normy PN-ISO/IEC 27002 pt. „Akceptowalne użycie aktywów" 8.1.3 oraz pt. „Postępowanie z aktywami" 8.2.3. W szczególności:
   a) dokumentacja może być udostępniona wyłącznie osobom mającym upoważnienie do dostępu do takiej informacji w oparciu o umowę z Centrum,
   b) Wykonawca jest zobowiązany do oznaczania dokumentacji projektowej klasą bezpieczeństwa według klasyfikacji Centrum,
   c) dokumentacja musi być przechowywana w repozytorium zapewniającym ochronę poufności oraz integralności przechowywanej dokumentacji,
   d) w przypadku gdy dokumentacja przetwarzana jest w repozytorium zarządzanym przez Wykonawcę, Wykonawca musi rejestrować zdarzenia związane z dostępem do bezpiecznego repozytorium i przechowywać bezpiecznie zapisy nie krócej niż 3 lata.

12. Bezpieczeństwo środowisk rozwojowych i testowych Wykonawcy

1. Wykonawca winien realizować prace rozwojowe z wykorzystaniem bezpiecznego środowiska rozwojowego, dla którego najlepsze praktyki określono w rozdziale normy PN-ISO/IEC 27002 pt. „Bezpieczne środowisko rozwojowe" (14.2.6). W szczególności Wykonawca musi zapewnić:
   a) zabezpieczenia środowiska rozwojowego i testowego adekwatne do poziomu ryzyka związanego z wykorzystaniem danych o określonym poziomie ochrony,
   b) kontrolę przepływu danych od i do środowiska rozwojowego i testowego, zapewniając brak upływu danych testowych oraz brak nieuprawnionego dostępu do systemów.
2. Wykonawca winien zapewnić bezpieczeństwo fizyczne środowisk rozwojowych i testowych zgodnie z najlepszymi praktykami określonymi w rozdziałach normy PN-ISO/IEC 27002 pt. „Obszary bezpieczne" 11.1 i „Sprzęt" 11.2. W szczególności Wykonawca musi:
   a) zapewnić bezpieczeństwo fizyczne obszaru, w którym znajdują środowiska rozwojowe i testowe,
   b) zapewnić ochronę fizyczną środowisk rozwojowych i testowych przed wrogim atakiem,
   c) zapewnić minimalizację ryzyk dotyczących środowisk rozwojowych i testowych związanych z nieuprawnionym dostępem.
   d) zapewnić bezpieczeństwo danych udostępnionych przez lub dotyczących Centrum w przypadku wynoszenia zasobów poza obszar chroniony.
3. Wykonawca winien zarządzać uprawnieniami dostępu do środowisk rozwojowych i testowych zgodnie z najlepszymi praktykami określonymi w rozdziałach normy PN-ISO/IEC 27002 pt. „Zarządzanie dostępem użytkowników" (9.2), pt. „Odpowiedzialność użytkowników" (9.3), pt. „Kontrola dostępu użytkowników do systemów i aplikacji" (9.4). W szczególności Wykonawca musi spełniać następujące wymagania:
   a) przyznawanie uprawnień dostępu do systemów rozwojowych i testowych musi być dokumentowane i kontrolowane,
   b) przyznawanie uprawnień do systemów rozwojowych i testowych musi być oparte o zasadę wiedzy koniecznej oraz zasadę potrzeby koniecznej,
   c) przyznawanie uprawnień musi zapewnić, że dostęp do danych chronionych i szczególnie chronionych uzyskają tylko te osoby, które są do tego upoważnione,
   d) przyznawanie uprawnień musi zapewnić możliwość rozliczalności użytkowników tych uprawnień,
   e) uprawnienia niewykorzystywane muszą być niezwłocznie odbierane,
   f) przyznane uprawnienia dostępu muszą podlegać kontroli nie rzadziej niż co 6 miesięcy, zaś wyniki przeglądów muszą być udokumentowane i przechowywane w bezpieczny sposób nie krócej niż 3 lata.
4. Wykonawca winien zapewnić (co najmniej na poziomie maszyny wirtualnej lub fizycznej) odseparowanie środowisk rozwojowych i testowych przeznaczonych do realizacji zadań na rzecz Centrum od środowisk realizujących zadania dla innych klientów, zgodnie z najlepszymi praktykami określonymi w rozdz. normy PN-ISO/IEC 27002 pt. „Oddzielanie środowisk rozwojowych, testowych, produkcyjnych" (12.1.4).
5. Wykonawca musi zapewnić rejestrowanie zdarzeń związanych z dostępem użytkowników oraz administratorów do systemów rozwojowych i testowych oraz zapewnić ich bezpieczne przechowywanie przez okres nie krótszy niż 2 lata[2]. Wykonawca musi udostępnić

[2] Zgodnie z ZSZ.SZBI.ISO.P.A.12.4._Polityka-logowania-zdarzen-zwiazanych-z-bezpieczenstwem_IW_v.1.0

przechowywane rejestry na życzenie Centrum w terminie 7 dni roboczych. Najlepsze praktyki w tym zakresie są określone w rozdziale normy PN-ISO/IEC 27002 pt. „Rejestrowanie zdarzeń i monitorowanie" (12.4).

6. Wykonawca musi zapewnić ochronę kopii zapasowych informacji przetwarzanej w trakcie realizacji zadań na rzecz Centrum, zgodnie z najlepszymi praktykami określonymi w rozdziale normy PN-ISO/IEC 27002 pt. „Kopie zapasowe" (12.3). W szczególności Wykonawca musi zapewnić fizyczne zabezpieczenie kopii bezpieczeństwa, a także gdy jest to właściwe dla wymaganego poziomu ochrony informacji, szyfrowanie kopii bezpieczeństwa.
7. Wykonawca musi zapewnić bezpieczeństwo danych testowych adekwatnie do rodzaju danych oraz klasy poufności tych danych, zgodnie z klasyfikacją Centrum.
8. Wykonawca musi zapewnić, że dostęp do danych testowych będą posiadały tylko osoby upoważnione. Wykorzystanie danych testowych musi być rejestrowane, zaś zapisy przechowywane przez okres co najmniej 3 lat.
9. Kody źródłowe muszą być przechowywane w bezpiecznym repozytorium kodów źródłowych, zgodnie z wymaganiami określonymi w rozdziale normy PN-ISO/IEC 27002 pt. „Kontrola dostępu do kodów źródłowych programów" (9.4.5).
10. W trakcie transferu kodów źródłowych Wykonawca musi zapewnić ich integralność oraz poufność, zgodnie z wymaganiami określonymi w rozdziale normy PN-ISO/IEC 27002 pt. „Porozumienia dotyczące przesyłania informacji" (13.2.2).
11. Wykonawca ma obowiązek zapewnić, że dostęp do repozytorium kodów źródłowych będzie kontrolowany, zaś korzystać z repozytorium będą osoby upoważnione. Dostęp do repozytorium musi zostać zarejestrowany, zaś rejestry przechowywane nie krócej niż 3 lata do daty zdarzenia.
12. Wykonawca ma obowiązek zapewnić, że wytworzone przez niego oprogramowanie spełnia wymagania standardu OWASP Application Security Verification Standard dla poziomu 2, chyba, że w Umowie wskazano inny poziom. W przypadku danych osobowych oczekiwanym jest spełnienie wymagań dla poziomu 3.

13. Incydenty bezpieczeństwa i naruszenia bezpieczeństwa danych osobowych

1. Wykonawca musi zapewnić identyfikowanie i obsługę incydentów bezpieczeństwa zgodnie z najlepszymi praktykami określonymi w rozdziale normy PN-ISO/IEC 27002 pt. „Zarządzanie incydentami związanymi z bezpieczeństwem informacji oraz udoskonaleniami" (16.1). W szczególności zobowiązany jest do niezwłocznego zgłaszania wszelkich zauważonych zdarzeń, które noszą znamiona lub są incydentami bezpieczeństwa oraz udzielania wszelkich niezbędnych informacji oraz wsparcia pracownikom Centrum zaangażowanym, z racji pełnionych obowiązków, w proces obsługi incydentu bezpieczeństwa.
2. W przypadku zaistnienia incydentu bezpieczeństwa Wykonawca musi podjąć wszelkie niezbędne środki, aby zminimalizować wpływ incydentu na działanie Centrum lub na jego wizerunek publiczny. Wykonawca musi także posiadać odpowiednie procedury umożliwiające gromadzenie wszelkich dowodów związanych z zaistnieniem incydentu bezpieczeństwa, zgodnie z najlepszymi praktykami określonymi w rozdziale normy PN-ISO/IEC 27002 pt. „Gromadzenie materiału dowodowego" (16.1.7).
3. Wszelkie zdarzenia wskazujące na naruszenie lub możliwość naruszenia zasad bezpieczeństwa informacji należy niezwłocznie zgłaszać: poprzez wiadomość e-mail na adres: incydent@cez.gov.pl.

4. W sytuacja pilnych wszelkie zdarzenia należy telefonicznie zgłaszać do dyżurnego operatora Centrum Operacji Bezpieczeństwa Centrum, pod numerem: **+48 501 369 699**.
5. Jeżeli naruszenie w jednoznaczny sposób dotyczy bezpieczeństwa przetwarzania danych osobowych, Wykonawca zobowiązany jest do bezpośredniego powiadomienia IOD. Zgłoszenia należy dokonać za pośrednictwem poczty elektronicznej, za potwierdzeniem odczytania, na adres: **iod@cez.gov.pl**, z tematem wiadomości „Naruszenie ochrony danych".
6. Zgłoszenie należy dokonać poprzez dedykowany formularz Podejrzenie Incydentu Bezpieczeństwa – Bezpieczeństwo – Projekt usługowy dostępny pod linkiem https://jirasd.csioz.gov.pl/servicedesk/customer/portal/21/create/501.
   Zgłoszenie to powinno zawierać. następujące informacje:
   a) imię i nazwisko zgłaszającego, dane kontaktowe (e-mail, telefon kontaktowy),
   b) nazwę podmiotu współpracującego (Wykonawcy),
   c) miejsce, data i czas wystąpienia zdarzenia,
   d) szczegółowy opis zdarzenia:
      - jakiego systemu, bądź aplikacji dotyczy zgłoszenie,
      - opis incydentu (dokładniejsze informacje),
      - czy incydent jest powtarzalny (występuje nieregularnie lub regularnie z określonym cyklem powtórzeń), ewentualny wpływ incydentu na funkcjonowanie systemu, w którym on wystąpił, oraz w systemach z nim powiązanych i zależnych,
      - wstępne skutki i oszacowanie szkód, jeśli doszło do materializacji takowych,
      - czy czynnik wywołujący incydent (na przykład intruz albo złośliwe oprogramowanie) został zidentyfikowany i czy jego aktywność nadal trwa,
      - komunikaty oraz logi systemowe w załącznikach (jeśli są dostępne),
      - ewentualnie zrzuty ekranowe w załącznikach.
7. Zgłaszający zdarzenie nie powinien podejmować żadnych działań na własną rękę, jednak w miarę możliwości powinien zabezpieczyć materiał dowodowy, np. wykonując zdjęcie ekranu co do którego zaistniało podejrzenie, że jego działanie odbiega od normy.
8. Jeśli zdarzenie ma miejsce w infrastrukturze zarządzanej przez Wykonawcę, upoważnione osoby ze strony Wykonawcy zabezpieczają ślady (np. logi systemowe).
9. Centrum zastrzega sobie prawo do zbierania i zabezpieczania wszelkich dowodów wskazujących na wystąpienie i powstanie skutków incydentu bezpieczeństwa, w szczególności prawo do wystąpienia do każdego z pracownika/współpracownika Wykonawcy z pisemnym żądaniem niezwłocznego włączenia się w obsługę incydentu bezpieczeństwa, w tym niezwłocznego podania wszelkich niezbędnych informacji w zakresie badanego incydentu bezpieczeństwa. O fakcie takiego wystąpienia wraz ze wskazaniem osób upoważnionych do żądania ww. informacji Centrum zobowiązana jest niezwłocznie powiadomić Wykonawcę.
10. Szczegółowy tryb postępowania w przypadku incydentu, regulują wewnętrzne procedury Zintegrowanego Systemu Zarządzania Centrum.
11. Każdorazowo, po zamknięciu incydentu, obsługujący incydent ze strony Centrum, zgodnie z procedurami wewnętrznymi sporządza Raport z incydentu oraz wydaje rekomendacje w zakresie działań zmierzających do zmniejszenia ryzyka powtórzenia incydentu w przyszłości, które przedstawiane są Wykonawcy wraz z potencjalnymi rekomendacjami wdrożenia wymaganych środków bezpieczeństwa.

14. Uprawnienia audytowe Centrum

1. Centrum zastrzega sobie prawo do przeprowadzenia audytów zgodności i bezpieczeństwa zastosowanych przez Wykonawcę rozwiązań organizacyjno-technicznych, zgodności zaimplementowanych mechanizmów bezpieczeństwa z obowiązującym prawem i niniejszą Polityką oraz sposobu korzystania przez personel Wykonawcy z udostępnionych im systemów lub zasobów teleinformatycznych Centrum. Wykonawca nie może odmówić przeprowadzenia audytu, w terminie wskazanym przez Centrum, zgodnie z pkt 4.
2. Wykonawca musi zapewnić Centrum możliwość przeprowadzenia audytów zgodności i bezpieczeństwa w zakresie świadczonych usług, bądź własnych środowisk rozwojowych i testowych wykorzystywanych do współpracy z Centrum, a także analogicznych środowisk własnych podwykonawców.
3. Wykonawca zobowiązany jest do umożliwienia przeprowadzenia audytu w szczególności poprzez:
   a) umożliwienie osobom audytującym wstępu do pomieszczeń Wykonawcy, w których jest wykonywana działalność związana z Umową,
   b) zapewnienie osobom audytującym dostępu do wszelkich wymaganych informacji, urządzeń oraz systemów teleinformatycznych wykorzystywanych do realizacji Umowy oraz personelu Wykonawcy i dokumentów w zakresie wynikającym z Umowy,
   c) udzielanie osobom audytującym przez osoby zaangażowane w realizację Umowy ze strony Wykonawcy wyjaśnień w żądanej formie - pisemnej lub ustnej w zakresie wynikającym z realizacji przedmiotu Umowy.
4. Audyt może być przeprowadzony w dni robocze, w godz. 9.00 – 16.00, w terminie ustalonym przez Centrum i przekazanym pisemnie do wiadomości Wykonawcy, z co najmniej 7-dniowym wyprzedzeniem.
5. W przypadku podejrzenia, bądź stwierdzenia rażącego naruszenia postanowień niniejszej Polityki przez personel Wykonawcy realizujący zadania na terenie Centrum, działania audytowe nie wymagają wcześniejszego powiadamiania Wykonawcy, i mogą być realizowane w dowolnym momencie.
6. Wyniki audytu winny być omówione z przedstawicielami Wykonawcy. Z przeglądu musi zostać sporządzony udokumentowany plan działania, w przypadku zidentyfikowania niezgodności.
7. W przypadku stwierdzenia uchybień w zakresie objętym audytem, Centrum ma prawo wezwać Wykonawcę do podjęcia działań w celu ich usunięcia w wyznaczonym terminie. Nie usunięcie uchybień w wyznaczonym terminie, może stanowić podstawę do wypowiedzenia Umowy.

15. Zakończenie umowy

1. Po zakończeniu realizacji Umowy, Wykonawca zobowiązany jest rozliczyć się z Centrum ze wszystkich otrzymanych aktywów powierzonych przez Centrum.
2. Jeśli Umowa nie stanowi inaczej, Wykonawca zobowiązany jest do zobligowania swych pracowników/współpracowników realizujących Umowę dla Centrum, do usunięcia wszelkich informacji stanowiących własność Centrum zapisanych na nośnikach, bądź urządzeniach Wykonawcy.
3. Wykonawca jest zobowiązany do zapewnienia bezpieczeństwa wszystkich informacji chronionych w okresie czasu określonym przez Umowę, po zakończeniu współpracy.

4. Wykonawca jest zobowiązany do skutecznego zniszczenia informacji, która winna zostać zniszczona po zakończeniu Umowy. Wykonawca jest zobowiązany do przedstawienia protokołu przeprowadzenia zniszczenia ww. informacji.

16. Postanowienia końcowe

1. Za nadzór nad przestrzeganiem postanowień niniejszej Polityki odpowiada:
   a) ze strony Wykonawcy, uprawniony przedstawiciel Wykonawcy,
   b) ze strony Centrum, Pełnomocnik ds. Zintegrowanego Systemu Zarządzania.
2. Naruszając zapisy niniejszej Polityki, Wykonawca może podlegać sankcjom karnym, cywilnym oraz wynikającym z przepisów art. 107 i art. 108 Ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych.

17. Dokumenty powiązane

1. ZSZ.ISO.P.01-Polityka_Dostepu_do_Srodowiska_Teleinformatycznego
2. Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r. poz. 1781 z późn. zm.)
3. Norma PN-ISO/IEC 27002 – Praktyczne zasady zabezpieczania informacji.
4. ZSZ.SZBI.ISO.P.A.11._Polityka-ochrony-fizycznej-obiektu_IW_v.1.0
5. ZSZ.SZBI.ISO.P.A.12.4._Polityka-logowania-zdarzen-zwiazanych-z-bezpieczenstwem_IW_v.1.0

18. Załączniki

1. ZSZ.SZBI.ISO.P.A.15.Z.1._Oswiadczenie-o-zapoznaniu-z-PBI-dla-wykonawcow_IP_v.1.1