



POLITYKA BEZPIECZEŃSTWA INFORMACJI DLA WYKONAWCÓW CENTRUM E-ZDROWIA

ZINTEGROWANY SYSTEM ZARZĄDZANIA

SPIS TREŚCI

1. Definicje i skróty.....	3
2. Wprowadzenie	4
2.1. Cel polityki	4
2.2. Zakres stosowania	4
2.3. Przeglądy i aktualizacja.....	4
2.4. Wyłączenia.....	4
3. Postanowienia ogólne	5
4. Zasady poruszania się Wykonawców w siedzibie CeZ.....	6
5. Dostęp do środowiska teleinformatycznego CeZ.....	6
5.1. Nadawanie, modyfikacja i wycofanie uprawnień.....	7
5.2. Odebranie dostępu.....	8
5.3. Metody i środki uwierzytelniania	8
6. Minimalne wymagania bezpieczeństwa	9
7. Bezpieczeństwo infrastruktury.....	11
8. Stosowanie zabezpieczeń kryptograficznych	12
9. Dostęp zdalny	12
10. Bezpieczeństwo środowisk produkcyjnych CeZ.....	14
11. Bezpieczeństwo prac projektowych Wykonawcy	15
12. Bezpieczeństwo środowisk rozwojowych i testowych Wykonawcy	15
13. Incydenty bezpieczeństwa i naruszenia bezpieczeństwa danych osobowych	17
14. Uprawnienia audytowe CeZ	19
15. Zakończenie umowy	20
16. Postanowienia końcowe.....	20
17. Dokumenty powiązane.....	21
18. Załączniki	21

1. Definicje i skróty

Autentyczność – atrybut bezpieczeństwa informacji dotyczący właściwości określającej, że jest ona wiarygodna.

CeZ, Centrum, Centrum e-Zdrowia - państwowa jednostka budżetowa, powołana przez Ministra Zdrowia, właściwa w zakresie systemów informacyjnych ochrony zdrowia.

Dostępność – atrybut bezpieczeństwa informacji zapewniający, że informacja jest dostępna uprawnionym, wtedy kiedy jest potrzebna.

Incydent bezpieczeństwa informacji (Incydent bezpieczeństwa) – pojedyncze zdarzenie lub seria niepożądanych, lub niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, które stwarzają znaczne prawdopodobieństwo zakłócenia działań biznesowych i zagrażają bezpieczeństwu informacji.

Integralność – atrybut bezpieczeństwa informacji dotyczący właściwości określającej, że żadna jej część nie została zniszczona lub zmodyfikowana przez nieuprawnione osoby.

Kod źródłowy – instrukcje w języku programowania czytelne dla człowieka, przekształcane w instrukcje maszynowe przez kompilator lub wykonywane przez interpreter.

OWASP ASVS – (ang Application Security Verification Standard) – zestaw wytycznych i poziomów weryfikacji bezpieczeństwa aplikacji.

Opiekun Osoby Trzeciej – wskazany przedstawiciel CeZ odpowiedzialny za nadzór nad stroną trzecią w tym umowy z nią zawarte.

Poufność – atrybut bezpieczeństwa informacji, który dotyczy właściwości określającej, że nie jest ona udostępniana osobom do tego nieupoważnionym.

Rozliczalność – możliwość weryfikacji kto i kiedy miał dostęp do danych informacji.

Tożsamość cyfrowa – zestaw danych, które w sposób unikalny opisują osobę i jej tożsamość, oraz zawierają informację na temat jej powiązań w systemach informatycznych.

Uwierzytelnienie – proces potwierdzenia tożsamości użytkownika, realizowany za pomocą metod takich jak: login i hasło (tradycyjna metoda uwierzytelniania), klucz sprzętowy, biometria, PIN.

Wykonawca (zewnętrzny) – podmiot gospodarczy powiązany umową formalnie-prawną z CeZ, realizujący dostawy lub świadczący usługi na rzecz CeZ.

ZSZ – Zintegrowany System Zarządzania zgodny z normą ISO 27001.

Polityka bezpieczeństwa informacji dla Wykonawców Centrum e-Zdrowia				
Wersja dokumentu:	1.3	Klauzula:	Do użytku publicznego	Strona 3 z 21

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 CeZ, a także bezpieczeństwa realizacji zadań na rzecz CeZ, poprzez m.in. określenie minimalnych wymagań w zakresie bezpieczeństwa informacji oraz zabezpieczeń systemów teleinformatycznych.

2.2. Zakres stosowania

Niniejsza Polityka obowiązuje wszystkich Wykonawców CeZ uzyskujących dostęp, przetwarzających, przechowujących, przesyłających lub dostarczających elementy infrastruktury teleinformatycznej dla przetwarzania informacji należących do CeZ. Niniejszy dokument dotyczy wszystkich systemów informatycznych, które są wdrażane, rozwijane bądź utrzymywane, będących własnością CeZ, 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 CeZ. 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 przepisy¹.

¹ Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz.U. 2025 poz. 1209 z późniejszymi zmianami).

Polityka bezpieczeństwa informacji dla Wykonawców Centrum e-Zdrowia				
Wersja dokumentu:	1.3	Klauzula:	Do użytku publicznego	Strona 4 z 21

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 CeZ. 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 CeZ.
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 CeZ, 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 CeZ 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.5.19.Z.1._Oswiadczenie-o-zapoznaniu-sie-z-Polityka-Bezpieczenstwa-Informacji-dla-Wykonawcow do niniejszej Polityki,
 - c) w przypadku powierzenia przetwarzania danych osobowych CeZ, podpisać umowę powierzenia przetwarzania danych osobowych zgodnie ze wzorem obowiązującym w CeZ.
4. Wykonawca winien zapewniać przez cały okres współpracy z CeZ, 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 CeZ, 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 CeZ. 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 CeZ nie może dochodzić do łączenia ról lub funkcji, które prowadziłyby do konfliktu interesów lub negatywnie wpływałyby na zabezpieczenie interesów CeZ.

Polityka bezpieczeństwa informacji dla Wykonawców Centrum e-Zdrowia				
Wersja dokumentu:	1.3	Klauzula:	Do użytku publicznego	Strona 5 z 21

4. Zasady poruszania się Wykonawców w siedzibie CeZ

1. Pracownikom Wykonawców wydawane są karty "Gość". Zasady wydawania i poruszania się po CeZ opisane są w Procedurze ochrony fizycznej obiektu.
2. Firmy mające stałe umowy i świadczące usługi w siedzibie CeZ są zobowiązane do zapoznania swoich pracowników z zasadami obowiązującymi w CeZ na podstawie Polityki ochrony fizycznej obiektu.
3. Powyższe punkty stosuje się w przypadku, gdy pracownik Wykonawcy musi przebywać na terenie CeZ.

5. Dostęp do środowiska teleinformatycznego CeZ

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 CeZ, polegającą w szczególności na zapewnieniu zespołu środków organizacyjnych, technicznych i prawnych stosowanych w celu zapewnienia bezpieczeństwa informacji.
3. Dostęp do krytycznych zasobów CeZ realizowany jest wyłącznie z użyciem stacji przesiadkowych udostępnianych przez CeZ. Sesje takie są izolowane, monitorowane i nagrywane w czasie rzeczywistym.
4. W związku z dostępem do środowiska teleinformatycznego CeZ, Wykonawca ma obowiązek stosować się do zaleceń oraz wymagań CeZ mających na celu zapewnienie bezpieczeństwa informacji, w tym m.in. zapoznać własny personel i zapewnić przestrzeganie wskazanych przez CeZ zasad bezpiecznego użytkowania systemu teleinformatycznego oraz zasad bezpiecznego użytkowania środowiska biurowego. Wykonawca jednocześnie zapewnia, że dostęp do systemów lub zasobów teleinformatycznych CeZ 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 CeZ oraz za wszelkie szkody powstałe w związku z korzystaniem przez Wykonawcę z dostępu do systemów lub zasobów teleinformatycznych CeZ 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 CeZ, o których mowa w niniejszej Polityce i ponosi w tym zakresie pełną odpowiedzialność względem CeZ.

8. Brak dostępu do systemów lub zasobów teleinformatycznych CeZ po stronie Wykonawcy, nie może być podstawą do dochodzenia od CeZ jakichkolwiek roszczeń.

5.1. Nadawanie, modyfikacja i wycofanie uprawnień

1. Dostęp Wykonawcy do środowiska teleinformatycznego CeZ 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 CeZ 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 CeZ, 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 CeZ 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.
6. Nadawanie, zmiana, bądź wycofanie uprawnień jest realizowane przez pracowników CeZ, zgodnie z poniższym schematem postępowania:
 - a) Opiekun Osoby Trzeciej, występuje o przydzielenie Tożsamości Cyfrowej dla Użytkowników będących personelem Wykonawcy, zgodnie z procedurami obowiązującymi w CeZ.
 - b) Na podstawie postanowień Umowy z Wykonawcą, Opiekun Osoby Trzeciej ustala niezbędny zakres uprawnień dla poszczególnych Użytkowników będących personelem Wykonawcy.
 - c) Opiekun Osoby Trzeciej występuje o nadanie, zmianę lub wycofanie uprawnień do systemu informatycznego, zgodnie z Polityką dostępu do środowiska teleinformatycznego.

- d) Administrator IT CeZ 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.
 - e) Po nadaniu, zmianie lub wycofaniu uprawnień w określonych systemach informatycznych, Administrator IT informuje o tym zdarzeniu Wykonawcę za pośrednictwem Opiekuna Osoby Trzeciej.
7. 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 CeZ 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 CeZ;
 - d) w wyniku decyzji Dyrektora Departamentu Bezpieczeństwa Teleinformatycznego 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 CeZ zagraża bezpieczeństwu informacji lub;
 - w przypadku stwierdzenia rażącego naruszenia przez Wykonawcę lub pracownika/współpracownika Wykonawcy postanowień niniejszej Polityki.

5.3. Metody i środki uwierzytelniania

Metody i środki uwierzytelniania takie jak:

- a) Login i polityka haseł, PIN
- b) Zasady dotyczące haseł dla kont użytkowników, administratorów IT, kont technicznych,
- c) Zasady stosowania biometrii i sprzętowych kluczy uwierzytelniających,

Polityka bezpieczeństwa informacji dla Wykonawców Centrum e-Zdrowia				
Wersja dokumentu:	1.3	Klauzula:	Do użytku publicznego	Strona 8 z 21

zostały opisane w rozdziale 8. Polityka uwierzytelniania w Polityce dostępu do środowiska teleinformatycznego (dostępnej dla Wykonawców po rozpoczęciu współpracy).

6. Minimalne wymagania bezpieczeństwa

1. Wykonawca musi zapewnić, że zadania realizowane na rzecz CeZ będą zarządzane zgodnie z najlepszymi praktykami określonymi w normie PN-ISO/IEC 27002 w rozdziale pt. „Bezpieczeństwo Informacji w zarządzaniu projektami” (A.5.8) 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 CeZ.
2. Wykonawca winien stosować klasyfikację informacji przesyłanej, przechowywanej i przetwarzanej w kontekście realizacji zadań na rzecz CeZ, zgodnie z zasadami klasyfikacji opisanymi w niniejszym dokumencie oraz najlepszymi praktykami określonymi w normie PN-ISO/IEC 27002 w rozdziale pt. „Klasyfikacja Informacji” (A.5.12).
3. Wykonawca jest zobowiązany do zapewnienia, przy dochowaniu najwyższej staranności, właściwej ochrony udostępnionego środowiska teleinformatycznego CeZ, 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 CeZ 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 CeZ,
 - podejmowanie działań, które pośrednio lub bezpośrednio mogą prowadzić do naruszenia bezpieczeństwa udostępnionych systemów lub zasobów teleinformatycznych.

Polityka bezpieczeństwa informacji dla Wykonawców Centrum e-Zdrowia				
Wersja dokumentu:	1.3	Klauzula:	Do użytku publicznego	Strona 9 z 21

5. Wykonawca musi zapewnić bezpieczeństwo informacji przesyłanej w związku z realizacją zadań na rzecz CeZ zgodnie z wymaganiami określonymi w rozdziale normy PN-ISO/IEC 27002 pt. „Przesyłanie informacji” (A.5.14). 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 CeZ. 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. „Outsourcing prac rozwojowych” (A.8.30) i „Zarządzanie bezpieczeństwem informacji w łańcuchu dostaw technologii informacyjno-komunikacyjnych (ICT)” (A.5.21).
7. Wykonawca winien zapewnić bezpieczeństwo wykorzystywanego personelu zgodnie z najlepszymi praktykami określonymi w rozdziałach norm PN-ISO/IEC 27002 pt. „Odpowiedzialność kierownictwa” (A.5.4), „Uświadamianie, kształcenie i szkolenia z zakresu bezpieczeństwa informacji” (A.6.3) oraz „Zakończenie zatrudnienia lub zmiana zakresu obowiązków” (A.6.5), adekwatnie do zadań realizowanych na rzecz CeZ. W szczególności, musi posiadać i realizować udokumentowane polityki dotyczące jego personelu, które obejmują:
 - a) przekazanie własnemu personelowi, realizującemu zadania na rzecz CeZ, informacji o wymaganiach bezpieczeństwa współpracy z CeZ,
 - b) wdrożenie programu cyklicznych szkoleń z zakresu bezpieczeństwa informacji i cyberbezpieczeństwa, a następnie zapewnienie udziału personelu oddelegowanego do współpracy z CeZ w tych szkoleniach.
8. Wykonawca musi zapewnić właściwe użycie aktywów, powierzonych przez CeZ, wykorzystywanych w pracach na rzecz CeZ zgodnie z najlepszymi praktykami określonymi w rozdziałach normy PN-ISO/IEC 27002 pt. „Akceptowalne użycie informacji i innych powiązanych aktywów” (A.5.10) i „Zwrot aktywów” (A.5.11). W szczególności wymagany 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 CeZ zgodnie z najlepszymi praktykami określonymi w rozdziale normy PN-ISO/IEC 27002 pt. „Zarządzanie nośnikami danych” (A.7.10). W szczególności musi:
 - a) posiadać i realizować polityki dotyczące bezpiecznego usuwania danych z nośników zawierających dane związane z realizacją zadań na rzecz CeZ, zapewniając skuteczne usuwanie,
 - b) posiadać i realizować polityki bezpiecznego przekazywania nośników zawierających dane związane z realizacją zadań na rzecz CeZ, 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 CeZ 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 Teleinformatycznego 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 CeZ do realizacji dostępu do środowiska teleinformatycznego CeZ, 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 CeZ nie mogą zagrażać bezpieczeństwu informacji. W szczególności Wykonawca zobowiązany jest do zastosowania odpowiednich zabezpieczeń chroniących przed złośliwym oprogramowaniem.

Polityka bezpieczeństwa informacji dla Wykonawców Centrum e-Zdrowia				
Wersja dokumentu:	1.3	Klauzula:	Do użytku publicznego	Strona 11 z 21

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 CeZ. 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 CeZ (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 CeZ, z wyłączeniem zadań realizowanych na mocy Umowy dotyczącej przeprowadzenia autoryzowanych testów bezpieczeństwa.
7. CeZ zastrzega sobie prawo do pełnej kontroli udostępnionych, jak i będących własnością Wykonawcy urządzeń, z których realizowany jest dostęp do środowiska teleinformatycznego CeZ.

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 CeZ,
 - 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.

Polityka bezpieczeństwa informacji dla Wykonawców Centrum e-Zdrowia				
Wersja dokumentu:	1.3	Klauzula:	Do użytku publicznego	Strona 12 z 21

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 CeZ pracy zdalnej oraz wykorzystywanych urządzeń mobilnych zgodnie z najlepszymi praktykami określonymi w rozdziale normy PN-ISO/IEC 27002 pt. „Urządzenia końcowe użytkowników” (A.8.1). 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 CeZ, zgodnie z najlepszymi praktykami określonymi w rozdziale normy pt. „Praca zdalna” (A.6.7). W szczególności:
 - a) dostęp do zasobów CeZ musi być realizowany wyłącznie z wykorzystaniem środowiska teleinformatycznego i informacji udostępnionych przez CeZ,
 - b) dostęp do zasobów CeZ musi być wykorzystywany tylko w celach i zakresie określonym przez CeZ,
 - c) przedstawiciele Wykonawcy posługują się wyłącznie indywidualnym loginem służącym do identyfikacji w systemach informatycznych CeZ; 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 Teleinformatycznego CeZ bezpośrednio, bądź poprzez Opiekuna Strony Trzeciej. Dalsze korzystanie ze zdalnego dostępu winno być realizowane wyłącznie po wyrażeniu zgody przez Departament Bezpieczeństwa Teleinformatycznego CeZ,

Polityka bezpieczeństwa informacji dla Wykonawców Centrum e-Zdrowia				
Wersja dokumentu:	1.3	Klauzula:	Do użytku publicznego	Strona 13 z 21

- h) osoby korzystające ze zdalnego dostępu muszą zapewnić, że zdalny komputer nie jest jednocześnie podłączony do innej sieci komputerowej, ewentualnie za wyjątkiem sieci komputerowej CeZ,
 - 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 Teleinformatycznego CeZ ma prawo do ciągłego monitorowania wszelkiej aktywności sieciowej w systemach należących do CeZ,
 - k) CeZ 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 Wi-Fi.
6. Zabrania się dostępu zdalnego z komputerów dostępnych publicznie (nie zarządzanych przez CeZ, bądź Wykonawcę), np. kawiarnie internetowe, dworce i lotniska itp.

10. Bezpieczeństwo środowisk produkcyjnych CeZ

1. W ramach dostępu zabrania się Wykonawcy trwale usuwać dane, przeprowadzać jakiegokolwiek 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 CeZ 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.

Polityka bezpieczeństwa informacji dla Wykonawców Centrum e-Zdrowia				
Wersja dokumentu:	1.3	Klauzula:	Do użytku publicznego	Strona 14 z 21

11. Bezpieczeństwo prac projektowych Wykonawcy

1. Wykonawca winien wykorzystywać w pracach projektowych, realizowanych na rzecz CeZ, najlepsze praktyki określone w rozdziałach normy PN-ISO/IEC 27002 pt. „Bezpieczeństwo prac rozwojowych” (A.8.25), „Zarządzanie zmianami” (A.8.32), „Zasady projektowania bezpiecznych systemów” (A.8.27). 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. „Monitorowanie, przegląd i zarządzanie zmianą usług świadczonych przez dostawców” (A.5.22). 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 CeZ, zgodnie z najlepszymi praktykami określonymi w rozdziale normy PN-ISO/IEC 27002 pt. „Akceptowalne użycie informacji i innych powiązanych aktywów” (A.5.10). W szczególności:
 - a) dokumentacja może być udostępniona wyłącznie osobom mającym upoważnienie do dostępu do takiej informacji w oparciu o umowę z CeZ,
 - b) Wykonawca jest zobowiązany do oznaczania dokumentacji projektowej klasą bezpieczeństwa według klasyfikacji CeZ,
 - 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

Polityka bezpieczeństwa informacji dla Wykonawców Centrum e-Zdrowia				
Wersja dokumentu:	1.3	Klauzula:	Do użytku publicznego	Strona 15 z 21

PN-ISO/IEC 27002 pt. „Rozdzielenie środowisk deweloperskich, testowych i produkcyjnych” (A.8.31). 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. „Praca w obszarach bezpiecznych” (A.7.6) i „Polityka czystego biurka i czystego ekranu” (A.7.7). 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 CeZ 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 tożsamością” (A.5.16), pt. „Prawa dostępu” (A.5.18), pt. „Uprzywilejowane prawa dostępu” (A.8.2), pt. „Informacje uwierzytelniające” (A.5.17), pt. „Ograniczenie dostępu do informacji” (A.8.3), pt. „Bezpieczne uwierzytelnianie” (A.8.5), pt. „Informacje uwierzytelniające” (A.5.17). 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 CeZ od środowisk realizujących zadania dla innych klientów,

Polityka bezpieczeństwa informacji dla Wykonawców Centrum e-Zdrowia				
Wersja dokumentu:	1.3	Klauzula:	Do użytku publicznego	Strona 16 z 21

zgodnie z najlepszymi praktykami określonymi w rozdz. normy PN-ISO/IEC 27002 pt. „Rozdzielenie środowisk deweloperskich, testowych i produkcyjnych” (A.8.31).

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 lata². Wykonawca musi udostępnić przechowywane rejestry na życzenie CeZ w terminie 7 dni roboczych. Najlepsze praktyki w tym zakresie są określone w rozdziale normy PN-ISO/IEC 27002 pt. „Rejestrowanie działań” (A.8.15).
6. Wykonawca musi zapewnić ochronę kopii zapasowych informacji przetwarzanej w trakcie realizacji zadań na rzecz CeZ, zgodnie z najlepszymi praktykami określonymi w rozdziale normy PN-ISO/IEC 27002 pt. „Zapasowe kopie bezpieczeństwa” (A.8.13). 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 CeZ.
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. „Dostęp do kodu źródłowego” (A.8.4).
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. „Przesyłanie informacji” (A.5.14).
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

² Zgodnie z ZSZ.SZBI.ISO.P.A.8.15._Polityka-logowania-zdarzen-zwiazanych-z-bezpieczenstwem_IW_v.1.0

Polityka bezpieczeństwa informacji dla Wykonawców Centrum e-Zdrowia				
Wersja dokumentu:	1.3	Klauzula:	Do użytku publicznego	Strona 17 z 21

pt. „Zgłaszanie zdarzeń związanych z bezpieczeństwem informacji” (A.6.08).

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 CeZ 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 CeZ 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 materiałów dowodowych” (A.5.28).
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 sytuacji pilnych wszelkie zdarzenia należy telefonicznie zgłaszać do dyżurnego operatora Centrum Operacji Bezpieczeństwa CeZ, 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 Podejrzanie 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.

Polityka bezpieczeństwa informacji dla Wykonawców Centrum e-Zdrowia				
Wersja dokumentu:	1.3	Klauzula:	Do użytku publicznego	Strona 18 z 21

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. CeZ 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 CeZ zobowiązana jest niezwłocznie powiadomić Wykonawcę.
10. Szczegółowy tryb postępowania w przypadku incydentu, regulują wewnętrzne procedury Zintegrowanego Systemu Zarządzania CeZ.
11. Każdorazowo, po zamknięciu incydentu, obsługujący incydent ze strony CeZ, 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 CeZ

1. CeZ 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 CeZ. Wykonawca nie może odmówić przeprowadzenia audytu, w terminie wskazanym przez CeZ, zgodnie z pkt 4.
2. Wykonawca musi zapewnić CeZ możliwość przeprowadzenia audytów zgodności i bezpieczeństwa w zakresie świadczonych usług, bądź własnych środowisk rozwojowych i testowych wykorzystywanych do współpracy z CeZ, 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

Polityka bezpieczeństwa informacji dla Wykonawców Centrum e-Zdrowia				
Wersja dokumentu:	1.3	Klauzula:	Do użytku publicznego	Strona 19 z 21

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 CeZ i przekazany 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 CeZ, 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, CeZ 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 CeZ ze wszystkich otrzymanych aktywów powierzonych przez CeZ.
2. Jeśli Umowa nie stanowi inaczej, Wykonawca zobowiązany jest do zobligowania swych pracowników/współpracowników realizujących Umowę dla CeZ, do usunięcia wszelkich informacji stanowiących własność CeZ 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 CeZ, Pełnomocnik ds. Zintegrowanego Systemu Zarządzania.

Polityka bezpieczeństwa informacji dla Wykonawców Centrum e-Zdrowia				
Wersja dokumentu:	1.3	Klauzula:	Do użytku publicznego	Strona 20 z 21

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. Polityka dostępu do środowiska teleinformatycznego
2. Norma PN-ISO/IEC 27002 – Zabezpieczanie informacji.
3. Polityka ochrony fizycznej obiektu
4. Polityka logowania zdarzeń związanych z bezpieczeństwem
5. Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r. poz. 1781 z późn. zm.)
6. 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) w zakresie zasad przetwarzania danych osobowych oraz zabezpieczania danych osobowych

18. Załączniki

1. ZSZ.SZBI.ISO.P.A.5.19.Z.1._Oswiadczenie-o-zapoznaniu-z-PBI-dla-wykonawcow_IP_v.1.2

Polityka bezpieczeństwa informacji dla Wykonawców Centrum e-Zdrowia				
Wersja dokumentu:	1.3	Klauzula:	Do użytku publicznego	Strona 21 z 21