

Zalecenia i wytyczne dla Użytkowników systemu CEPiK 2.0 w zakresie bezpieczeństwa i ochrony danych osobowych

wersja z dnia 15 czerwca 2016 r.

Spis treści

1. Wprowadzenie	4
2. Poziom bezpieczeństwa	4
3. Kategorie użytkowników	4
4. Użytkownicy Instytucjonalni.....	6
4.1. Dokumentacja opisująca sposób przetwarzania danych osobowych	6
4.2. Środki ochrony kryptograficznej	7
4.3. Połączenie z systemem CEPiK 2.0	7
4.4. Rozliczalność	8
4.5. Podpisywanie komunikatów	8
5. Zalecenia i wytyczne dla Użytkowników Instytucjonalnych w zakresie ochrony danych osobowych.....	8
5.1. Ochrona fizyczna	9
5.1.1. Pomieszczenia i ich lokalizacja	9
5.1.2. Kontrola dostępu do pomieszczeń	9
5.1.3. Zabezpieczenie drzwi i okien.....	10
5.2. Zabezpieczenia urządzeń oraz nośników danych	10
5.2.1. Nośniki danych i informacji	10
5.2.2. Urządzenia służące do nawiązywania komunikacji za pomocą sieci dedykowanych....	11
5.2.3. Urządzenia i oprogramowanie służące do nawiązania połączeń VPN przez sieć publiczną Internet	11
5.2.4. Sprzęt komputerowy stacjonarny	12
5.2.5. Środowiska wirtualne (maszyny wirtualne).....	16
5.2.6. Sprzęt komputerowy przenośny (laptop, tablet, itp.)	16
6. Użytkownicy Indywidualni.....	19
6.1. Dokumentacja opisująca sposób przetwarzania danych osobowych	19
6.2. Środki ochrony kryptograficznej	20
6.3. Połączenie z systemem CEPiK 2.0	20
6.4. Rozliczalność	21
6.5. Podpisywanie komunikatów	21
7. Zalecenia i wytyczne dla Użytkowników Indywidualnych w zakresie ochrony danych osobowych	21
7.1. Ochrona fizyczna	21
7.1.1. Pomieszczenia i ich lokalizacja	21
7.1.2. Kontrola dostępu do pomieszczeń	22

7.1.3.	Zabezpieczenie drzwi i okien.....	22
7.2.	Zabezpieczenia urządzeń oraz nośników danych	23
7.2.1.	Nośniki danych i informacji	23
7.2.2.	Urządzenia służące do nawiązywania komunikacji za pomocą sieci dedykowanych....	23
7.2.3.	Urządzenia i oprogramowanie służące do nawiązania połączeń VPN przez sieć publiczną Internet	24
7.2.4.	Sprzęt komputerowy stacjonarny	24
7.2.5.	Środowiska wirtualne (maszyny wirtualne).....	28
7.2.6.	Sprzęt komputerowy przenośny (laptop, tablet, itp.)	29
8.	Wnioskowanie o dostęp do systemu CEPiK 2.0	31
8.1.	Podmioty określone w art. 80ba. ust. 1 ustawy PoRD – zasilanie centralnej ewidencji pojazdów	31
8.2.	Podmioty określone w art. 80c. ust. 1 ustawy PoRD – dostęp do centralnej ewidencji pojazdów	31
8.3.	Podmioty określone w art. 100 ac. ust. 1 ustawy PoRD – zasilanie centralnej ewidencji kierowców	31
8.4.	Podmioty określone w art. 100 ah. ust. 1 ustawy PoRD – dostęp do centralnej ewidencji kierowców	31
8.5.	Podmioty określone w art. 100g ust. 2 ustawy PoRD – zasilanie centralnej ewidencji posiadaczy kart parkingowych	32
8.6.	Podmioty określone w art. 100 k. ust. 1 ustawy PoRD – dostęp do centralnej ewidencji posiadaczy kart parkingowych	32
8.7.	Pozostałe podmioty	32
8.8.	Wnioskowanie	32
9.	Incydenty bezpieczeństwa.....	33
10.	Audyty.....	33

1. Wprowadzenie

Każdy Użytkownik systemu CEPiK 2.0 zobowiązany jest do ochrony danych osobowych, zgodnie z obowiązującymi w tym zakresie przepisami prawa. Użytkownik jest zobowiązany do wytworzenia dokumentacji opisującej sposób ochrony tych danych oraz wdrożyć środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, w szczególności powinien zabezpieczyć dane osobowe przed ich udostępnieniem osobom nieupoważnionym, zabranieniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.

2. Poziom bezpieczeństwa

System informatyczny CEPiK 2.0 jest systemem z zaimplementowanymi środkami bezpieczeństwa na poziomie wysokim¹. Każdy Użytkownik systemu CEPiK 2.0 obowiązany jest stosować środki bezpieczeństwa na poziomie wysokim, z zastrzeżeniem Stacji Kontroli Pojazdów, dla których wymagania i zalecenia zostały określone w osobnym rozdziale niniejszego dokumentu.

3. Kategorie użytkowników

Użytkownikiem systemu CEPiK 2.0 jest każdy podmiot uprawniony do dostępu do systemu i posiadający w systemie konto identyfikujące dany podmiot, oraz każda osoba uprawniona do dostępu do systemu posiadająca w systemie spersonalizowane konto. W systemie CEPiK 2.0 wyróżnia się następujące kategorie użytkowników:

- Użytkownicy Instytucjonalni (UI),
 - Stacje Kontroli Pojazdów,
- Użytkownicy Indywidualni (UIn),
- Administratorzy Systemu Informatycznego CEPiK 2.0 (ASI).

Użytkownicy Instytucjonalni to kategoria użytkowników obejmująca podmioty uprawnione do dostępu do danych przetwarzanych w systemie CEPiK 2.0, które do komunikacji z systemem CEPiK 2.0 wykorzystują własne systemy i aplikacje. Integracja z systemem CEPiK 2.0 jest realizowana przez integrację tych systemów i aplikacji z interfejsami API i usługami web services systemu CEPiK 2.0.

Wydzieloną podgrupą Użytkowników Instytucjonalnych są podmioty takie jak stacje kontroli pojazdów, które ze względu na swoją specyfikę działania oraz obowiązujące przepisy prawa m.in. ustawę Prawo o ruchu drogowym, nie są uprawnione do dostępu do danych osobowych. W związku z tym wymagany dla tych podmiotów poziom zabezpieczeń jest odpowiednio ograniczony, mając na uwadze specyfikę danych podlegających ochronie oraz ogólne uwarunkowania systemu CEPiK 2.0 i infrastruktury prywatnej chmury obliczeniowej, w której system ten funkcjonuje.

Użytkownicy Indywidualni to kategoria użytkowników obejmująca osoby uprawnione do dostępu do danych przetwarzanych w systemie CEPiK 2.0, które korzystają z aplikacji przeglądarkowej (tzw. cienkiego klienta) udostępnianej przez system CEPiK 2.0 w celu dostępu do tego systemu.

¹ Środki bezpieczeństwa na poziomie wysokim zgodnie z rozporządzeniem Ministra Spraw Wewnętrznych i Administracji w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

Administratorzy Systemu Informatycznego CEPiK 2.0 to specjalna kategoria użytkowników, którzy są odpowiedzialni za utrzymanie i eksploatację systemu CEPiK 2.0.

4. Użytkownicy Instytucjonalni

Niniejszy rozdział dotyczy Użytkowników Instytucjonalnych, którzy korzystają z własnych systemów i aplikacji do komunikacji z systemem CEPiK 2.0.

4.1. Dokumentacja opisująca sposób przetwarzania danych osobowych

Każdy Użytkownik Instytucjonalny systemu CEPiK 2.0 z chwilą pozyskania danych osobowych z systemu CEPiK staje się administratorem tych danych. Zgodnie z art. 36 ust 1 *ustawy o ochronie danych osobowych* administrator danych obowiązany zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabranieniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem. Zgodnie z art. 36 ust 2 tej ustawy administrator danych prowadzi dokumentację opisującą sposób przetwarzania danych oraz środki wskazane w zdaniu poprzednim.

Zgodnie z § 3 ust. 1 *rozporządzenia Ministra Spraw Wewnętrznych i Administracji w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych*, na dokumentację, o której mowa w poprzednim akapicie, składa się polityka bezpieczeństwa i instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

Polityka bezpieczeństwa zawiera w szczególności (zgodnie z § 4 ww. rozporządzenia):

1. wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe,
2. wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych,
3. opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi,
4. sposób przepływu danych pomiędzy systemami,
5. środki techniczne i organizacyjne niezbędne do zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.

Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych zawiera w szczególności (zgodnie z § 5 ww. rozporządzenia):

1. procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynność,
2. stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem,
3. procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu,
4. procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania,
5. sposób, miejsce i okres przechowywania:
 - a. elektronicznych nośników informacji zawierających dane osobowe,

- b. kopii zapasowych, o których mowa w pkt 4,
6. sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego,
7. sposób realizacji wymogów w zakresie odnotowywania informacji związanych z przetwarzaniem danych osobowych takich jak: data wprowadzenia danych, identyfikator użytkownika wprowadzającego dane, źródła danych, informacji o odbiorcach danych, w tym dacie i zakresie udostępnionych danych,
8. procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych.

Każdy Użytkownik Instytucjonalny, z chwilą podłączenia do systemu CEPiK 2.0, zobowiązany jest do posiadania wskazanej powyżej dokumentacji.

4.2.Środki ochrony kryptograficznej

W systemie CEPiK 2.0 stosowane są środki kryptograficznej ochrony danych. Każdy Użytkownik Instytucjonalny musi posiadać odpowiedni certyfikat, aby móc skorzystać z usług systemu CEPiK 2.0. Szczegółowy sposób uzyskania certyfikatów, ich wymiany, sposób ochrony kluczy prywatnych oraz inne informacje i wymagania związane z certyfikatami są opisane w dokumentach:

- Polityka certyfikacji dla infrastruktury systemu informatycznego CEPiK 2.0;
- Polityka certyfikacji dla operatorów systemu informatycznego CEPiK 2.0;
- Polityka certyfikacji dla ADSxP.

W ramach polityki certyfikacji dla infrastruktury systemu informatycznego CEPiK 2.0 wydawane są certyfikaty dla systemów zewnętrznych służące do autoryzacji, uwierzytelniania, podpisywania komunikatów i zestawiania SSL (certyfikaty SSL), oraz certyfikaty służące do zestawiania połączeń VPN (certyfikaty VPN).

W ramach polityki certyfikacji dla operatorów systemu informatycznego CEPiK 2.0 wydawane są certyfikaty dla użytkowników aplikacji przeglądarkowych udostępnianych przez system CEPiK 2.0 służące do autoryzacji, uwierzytelniania, podpisywania komunikatów i zestawiania SSL (certyfikaty SSL).

W systemach teleinformatycznych organów właściwych w sprawach rejestracji pojazdów oraz organów właściwych w sprawach wydawania dokumentów stwierdzających uprawnienia do kierowania pojazdami, każdy użytkownik końcowy tych systemów musi posługiwać się certyfikatem SSL służącym do autoryzacji, uwierzytelniania, podpisywania komunikatów i zestawiania SSL (certyfikaty SSL). Certyfikaty użytkowników końcowych tych systemów wydawane są w polityce certyfikacji dla ADSxP – są to spersonalizowane certyfikaty, każdy przypisany do konkretnej osoby.

4.3.Połączenie z systemem CEPiK 2.0

Użytkownik Instytucjonalny ma możliwość połączenia się z systemem CEPiK 2.0 przez sieć publiczną Internet oraz przez sieć wydzieloną np. OST112, GovNet, sTesta, PESEL-NET.

Użytkownik Instytucjonalny łączący się z systemem CEPiK 2.0 przez sieć publiczną Internet musi zestawić bezpieczne połączenie VPN z wykorzystaniem certyfikatu VPN. Dopiero po zestawieniu połączenia VPN użytkownik ma możliwość wywołania usług systemu CEPiK. Autoryzacja i

uwierzytelnienie Użytkownika w usługach systemu CEPiK 2.0 są realizowane w oparciu o posiadany przez Użytkownika certyfikat SSL.

Użytkownik łączący się z systemem CEPiK przez sieć wydzieloną ma możliwość wywołania usług systemu CEPiK bez konieczności zestawiania bezpiecznego połączenia VPN – autoryzacja i uwierzytelnienie Użytkownika w usługach systemu CEPiK są realizowane w oparciu o posiadany przez Użytkownika certyfikat SSL.

System CEPiK 2.0 wspiera rozwiązania programowe Cisco VPN Client oraz Cisco AnyConnect i komunikację VPN typu Remote Access. Dla tych rozwiązań Service Desk zapewni wsparcie związane z instalacją oraz konfiguracją oprogramowania. Rozwiązanie VPN typu Remote Access będzie wymuszało politykę bezpieczeństwa sieci, m.in. po zestawieniu połączenia VPN dostęp do zasobów sieci publicznej Internet będzie ograniczony, możliwe będzie wywoływanie usług CEPiK 2.0.

System CEPiK 2.0 dopuszcza połączenia VPN typu Lan-to-Lan, przy czym ich nie wspiera. Każdy Użytkownik Instytucjonalny decydujący się na takie połączenie powinien je zestawić we własnym zakresie, na podstawie wskazanych do zastosowania parametrów konfiguracyjnych. Przed implementacją takiego rozwiązania należy skontaktować się z Service Desk CEPiK w celu otrzymania niezbędnych danych i informacji, które umożliwią konfigurację urządzeń po stronie użytkownika.

4.4.Rozliczalność

System CEPiK 2.0 zapewnia pełną rozliczalność działań Użytkowników Instytucjonalnych w systemie, w szczególności w zakresie operacji wykonywanych na danych osobowych. Każde działanie użytkownika podlega odnotowaniu w podsystemie logowania CEPiK 2.0. Użytkownik Instytucjonalny jest identyfikowany w oparciu o certyfikat SSL wydany dla systemu teleinformatycznego Użytkownika Instytucjonalnego. Dodatkowo system zewnętrzny Użytkownika Instytucjonalnego musi przekazywać do systemu CEPiK 2.0, w przekazywanych komunikatach, identyfikator użytkownika końcowego tego systemu, który wykonuje operacje na danych osobowych w systemie CEPiK 2.0. Szczegółowy sposób przekazywania identyfikatora użytkownika jest określony w dokumentacji opisującej sposób działania usług web services systemu CEPiK 2.0.

Niezależnie od powyższego, rozliczalność działań użytkownika końcowego jest zobowiązaniem Użytkownika Instytucjonalnego i musi być zaimplementowana w systemie teleinformatycznym, który komunikuje się z systemem CEPiK 2.0.

4.5.Podpisywanie komunikatów

Każdy komunikat przekazywany do systemu CEPiK 2.0 przez system zewnętrzny lub aplikację Użytkownika Instytucjonalnego musi być opatrzony podpisem elektronicznym. Szczegółowe wymagania związane z podpisywaniem komunikatów są określone w dokumentacji opisującej sposób działania usług web services systemu CEPiK 2.0.

5. Zalecenia i wytyczne dla Użytkowników Instytucjonalnych w zakresie ochrony danych osobowych

Niniejszy rozdział opisuje wytyczne dla Użytkowników Instytucjonalnych w zakresie ochrony danych osobowych. Użytkownik Instytucjonalny może wykorzystać poniższe zalecenia w celu opracowania własnej dokumentacji, o której mowa w pkt. 4.1.

W przypadku, gdy użytkownik posiada już dokumentację, o której mowa w pkt. 4.1 zakłada się, że Użytkownik zastosował wytyczne i zalecenia co najmniej na poziomie minimalnym.

W przypadku, gdy system Użytkownika został dopuszczony przez właściwą służbę ochrony państwa do przetwarzania informacji niejawnych, po uzyskaniu certyfikatu wydanego na podstawie przepisów ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych zakłada się, że zastosowane są wytyczne i zalecenia na poziomie zalecanym.

5.1.Ochrona fizyczna

Niniejszy rozdział opisuje wytyczne w zakresie ochrony fizycznej pomieszczeń, w których będą przetwarzane dane osobowe, oraz ochrony fizycznej urządzeń wykorzystywanych do przetwarzania danych osobowych, które będą zlokalizowane w tych pomieszczeniach.

5.1.1. Pomieszczenia i ich lokalizacja

5.1.1.1. Poziom minimalny

- Pomieszczenia, w których będą przetwarzane dane osobowe, powinny zapewniać takie rozmieszczenie urządzeń oraz dokumentów, aby uniemożliwić dostęp (m.in. wgląd, podejrzenie) do danych osobowych osobom nieuprawnionym do dostępu do tych danych, np. przez zastosowanie wygradzeń, żaluzji, odpowiednie ustawienie monitora względem okna i drzwi.
- Pomieszczenia, w których będą przetwarzane dane osobowe, powinny być zlokalizowane w miejscach, gdzie ryzyko ich zatopienia lub zalania jest zminimalizowane.

5.1.1.2. Poziom zalecany

- Pomieszczenia, w których będą przetwarzane dane osobowe, powinny zapewniać takie rozmieszczenie urządzeń oraz dokumentów, aby uniemożliwić dostęp (m.in. wgląd, podejrzenie) do danych osobowych osobom nieupoważnionym do dostępu do tych danych, np. przez zastosowanie wygradzeń, żaluzji, odpowiednie ustawienie monitora względem okna i drzwi.
- Pomieszczenia, w których będą przetwarzane dane osobowe, nie powinny być pomieszczeniami przechodnimi.
- Pomieszczenia, w których będą przetwarzane dane osobowe, powinny być wyposażone w system alarmowy, system przeciwpożarowy, np. czujniki zadymienia wraz z funkcją powiadomienia do służby ochrony lub jednostek straży pożarnej, policji.

5.1.2. Kontrola dostępu do pomieszczeń

5.1.2.1. Poziom minimalny

- Zaleca się w przypadku braku systemu elektronicznej kontroli dostępu, wdrożenie manualnej kontroli dostępu do pomieszczeń, w których będą przetwarzane dane osobowe, w sposób organizacyjny – proceduralny, np. książka pobrań kluczy.
- Dostęp do pomieszczeń, w których będą przetwarzane dane osobowe, powinny posiadać wyłącznie osoby uprawnione.
- Jeżeli istnieje taka konieczność, inne osoby mogą przebywać w tych pomieszczeniach jedynie w obecności osób uprawnionych, za ich wiedzą i zgodą.

5.1.2.2. Poziom zalecany

- Zaleca się zastosowanie systemu elektronicznej kontroli dostępu do pomieszczeń, w których będą przetwarzane dane osobowe.
- Urządzenia automatycznej kontroli dostępu winny być nadzorowane całodobowo przez służbę ochrony.
- Zaleca się wdrożenie procedury cyklicznego sprawdzenia logów systemu elektronicznej kontroli dostępu do pomieszczeń.
- Dostęp do pomieszczeń powinny posiadać wyłącznie osoby uprawnione.
- Jeżeli istnieje taka konieczność, inne osoby mogą przebywać w tych pomieszczeniach jedynie w obecności osób uprawnionych, za ich wiedzą i zgodą.
- Zaleca się stosowanie systemu elektronicznej kontroli dostępu do pomieszczeń w celu odnotowania wejść osób nieuprawnionych lub zastosowanie środków organizacyjno – proceduralnych, np. odnotowywanie wejść osób nieuprawnionych w książce wejść.

5.1.3. Zabezpieczenie drzwi i okien

5.1.3.1. Poziom minimalny

- Drzwi do pomieszczeń, w których będą przetwarzane dane osobowe, powinny być zabezpieczone przed wyważeniem (podważeniem) oraz wyposażone w bezpieczny zamek.
- Otwory okienne pomieszczeń zlokalizowanych na parterze lub ostatniej kondygnacji (o ile jest swobodny dostęp do dachu) powinny być okratowane lub zabezpieczone w inny, równoważny sposób (np. folią antywłamaniową).

5.1.3.2. Poziom zalecany

- Drzwi do pomieszczeń, w których będą przetwarzane dane osobowe, znajdujących się wewnątrz budynku w strefie ograniczonego dostępu (bądź strefie dozorowanej) powinny być zabezpieczone przed wyważeniem i wyposażone w co najmniej 1 zamek atestowany (klasa C).
- Drzwi znajdujące się wewnątrz budynku w strefie ogólnodostępnej niedozorowanej powinny spełniać wymagania co najmniej klasy 2 zgodnie z normą PN-EN14351-1+A1:2010 oraz być wyposażone w co najmniej jeden zamek atestowany (klasa C).
- Drzwi, do których dostęp jest z zewnątrz budynku, powinny spełniać wymagania co najmniej klasy 3 zgodnie z normą PN-EN14351-1+A1:2010.
- Otwory okienne pomieszczeń zlokalizowanych na parterze lub ostatniej kondygnacji (o ile jest swobodny dostęp do dachu) powinny być okratowane lub posiadać okna spełniające wymagania co najmniej klasy 2 zgodnie z normą PN-EN14351-1+A1:2010 z szybą klasy P4.

5.2. Zabezpieczenia urządzeń oraz nośników danych

5.2.1. Nośniki danych i informacji

5.2.1.1. Poziom minimalny

- Dokumenty i nośniki informacji zawierające dane osobowe powinny być przechowywane w miejscu uniemożliwiającym dostęp do nich osobom nieupoważnionym (np. w zamykanych na klucz szafkach).
- Do likwidacji wydruków dokumentów i nośników informacji powinno się stosować przeznaczone do tego celu niszczarki.

5.2.1.2. Poziom zalecany

- Dane przechowywane na elektronicznych oraz papierowych nośnikach danych powinny być składowane w szafach wyposażonych w co najmniej 1 zamek atestowany (klasa A).
- Do likwidacji wydruków dokumentów i nośników informacji powinno się stosować niszczarki klasy DIN 3 zgodnie z normą DIN 32757.

5.2.2. Urządzenia służące do nawiązywania komunikacji za pomocą sieci dedykowanych

5.2.2.1. Zalecenia w zakresie konfiguracji urządzeń

- Użytkownicy łączący się z systemem CEPiK poprzez sieci dedykowane powinni stosować się do wymagań i zaleceń określonych dla konkretnej sieci dedykowanej.
- Urządzenia sieciowe (takie jak routery oraz przełączniki sieciowe) pozwalające na dostęp do sieci dedykowanej powinny być zabezpieczone przed nieuprawnionym dostępem osób trzecich:
 - Administracja zdalna powinna być odpowiednio zabezpieczona przed nieuprawnionym dostępem za pomocą mechanizmów uwierzytelnienia routera (np. login i hasło o odpowiedniej złożoności).
 - Administracja zdalna powinna być uruchomiona wyłącznie na jednym porcie wewnętrznym, do którego ma dostęp wyłącznie administrator danego urządzenia.
 - Powinna być wdrożona reglamentacja dostępu do sieci np. na podstawie adresów MAC.

5.2.2.2. Zalecenia w zakresie bezpieczeństwa fizycznego urządzeń

- Urządzenia sieciowe powinny być zlokalizowane w pomieszczeniu lub szafie z ograniczonym dostępem osób trzecich. Dostęp do tego pomieszczenia lub szafy powinien mieć wyłącznie administrator urządzenia lub osoby upoważnione.

5.2.3. Urządzenia i oprogramowanie służące do nawiązania połączeń VPN przez sieć publiczną Internet

5.2.3.1. Zalecenia w zakresie konfiguracji urządzeń i oprogramowania

- Użytkownicy łączący się z systemem CEPiK poprzez sieć publiczną Internet, aby uzyskać dostęp do systemu CEPiK, muszą zestawić bezpieczne połączenie VPN z wykorzystaniem certyfikatu.
- Urządzenia sieciowe (takie jak routery) pozwalające na zestawienie połączeń VPN powinny być zabezpieczone przed nieuprawnionym dostępem osób trzecich:
 - Urządzenie powinno być zabezpieczone w sposób uniemożliwiający osobom nieuprawnionym pozyskanie kluczy prywatnych do certyfikatu VPN, zainstalowanych w urządzeniu.
 - Administracja zdalna powinna być odpowiednio zabezpieczona przed nieuprawnionym dostępem za pomocą mechanizmów uwierzytelnienia routera (np. login i hasło o odpowiedniej złożoności).
 - Administracja zdalna powinna być uruchomiona wyłącznie na jednym porcie wewnętrznym, do którego ma dostęp wyłącznie administrator danego urządzenia.
 - Powinna być wdrożona reglamentacja dostępu do sieci np. na podstawie adresów MAC.

- Powinna być wdrożona polityka blokowania dostępu do i z sieci publicznej Internet w czasie, w którym jest nawiązane połączenie VPN.
- Oprogramowanie służące do zestawiania połączeń VPN (typu Remote Access) powinno być zabezpieczone w taki sposób, aby uniemożliwić dostęp do kluczy prywatnych osobom nieuprawnionym.
- Oprogramowanie służące do zestawiania połączeń VPN (typu Remote Access) powinno wymuszać blokowanie dostępu do i z sieci publicznej Internet do danej stacji komputerowej w czasie, w którym jest nawiązane połączenie VPN (jest to wymuszone przez konfigurację urządzeń po stronie systemu CEPiK).

5.2.3.2. *Zalecenia w zakresie bezpieczeństwa fizycznego urządzeń*

- Urządzenia sieciowe powinny być zlokalizowane w pomieszczeniu lub szafie z ograniczonym dostępem osób trzecich. Dostęp do tego pomieszczenia lub szafy powinien mieć wyłącznie administrator urządzenia lub osoby upoważnione.

5.2.4. Sprzęt komputerowy stacjonarny

5.2.4.1. *Poziom minimalny*

- Zaleca się wprowadzenie w BIOS następujących ustawień:
 - wejście i zmiana ustawień BIOS wymaga podania hasła,
 - wyłączona jest możliwość uruchamiania systemu z sieci lub innych nośników niż dysk twardy komputera,
 - długość hasła BIOS powinna wynosić nie mniej niż 6 znaków (co najmniej 1 duża litera i 1 cyfra).
- Konta użytkowników i hasła:
 - wbudowane konto administratora powinno być używane tylko w przypadku wykonywania czynności administratora,
 - każdemu użytkownikowi komputera powinno być założone oddzielne konto, konta te nie powinny mieć przypisanych uprawnień administratora, o ile nie jest to wymagane do bieżącej pracy,
 - długość nazwy użytkownika powinna wynosić nie mniej niż 3 znaki,
 - długość hasła konta administratora lub użytkownika z uprawnieniami administratora powinna wynosić nie mniej niż 10 znaków (hasło złożone co najmniej 1 duża litera, 1 cyfra i znak specjalny), okres ważności hasła nie powinien być dłuższy niż 30 dni,
 - długość hasła konta użytkownika powinna wynosić nie mniej niż 8 znaków (hasło złożone co najmniej 1 duża litera, 1 cyfra i znak specjalny), okres ważności hasła nie dłuższy niż 30 dni,
 - zaleca się wprowadzić regulacje sankcjonujące zmianę pin-kodu mikroprocesorowych kart kryptograficznych nie rzadziej niż co 30 dni,
 - zaleca się wprowadzić stosowne regulacje sankcjonujące sposoby przechowywania nazw użytkowników i haseł oraz zabraniające udostępnia ich innym osobom.
- Ochrona przed atakami zewnętrznymi (zapora ogniowa):
 - zalecane jest zastosowanie zapory ogniowej (sprzętowej lub programowej) oraz wdrożenie regulacji zapewniających jej bieżącą aktualizację.
- Sieci Wi-Fi:

- do połączenia z sieciami Wi-Fi zaleca się używać co najmniej standardu WPA i haseł o długości nie mniejszej niż 12 znaków (hasło złożone co najmniej 1 duża litera, 1 cyfra i znak specjalny).
- Ochrona antywirusowa:
 - zalecane jest zainstalowanie oprogramowania antywirusowego oraz wdrożenie regulacji zapewniających aktualizację sygnatur antywirusowych nie rzadziej niż raz w tygodniu,
 - zalecane jest wdrożenie regulacji zapewniających pełne skanowanie antywirusowe stacji co najmniej 1 raz w tygodniu w przypadku braku ochrony w czasie rzeczywistym i nie mniej niż 1 raz w miesiącu w przypadku stosowania ochrony w czasie rzeczywistym.
- Aktualizacja systemu i oprogramowania:
 - zalecane jest stosowanie systemów operacyjnych w wersjach wspieranych przez ich producentów,
 - zalecane jest wdrożenie regulacji związanych z aktualizowaniem systemu operacyjnego oraz wykorzystywanego oprogramowania zgodnie z zaleceniami producentów.
- Usuwanie danych:
 - zaleca się konfigurację „kosza” systemowego, aby nie przechowywał usuniętych plików.
- Dyski i urządzenia przenośne:
 - w przypadku stosowania dysków twardych umieszczonych w wyjmowanych kieszeniach powinny być one wyposażone w zamknięcie na kluczyk i zamknięte, gdy znajduje się w nich dysk. Po zakończonej pracy zalecane jest usunięcie dysku i jego dalsze przechowywanie w zabezpieczonej szafie,
 - powinny być wdrożone regulacje zapewniające obsługę pamięci flash, oraz dysków przenośnych, podłączanych okresowo do stacji, zawierających dane, tak aby po zakończeniu pracy były one usuwane ze stacji i przechowywać w bezpieczny sposób,
 - przenośne pamięci flash oraz dyski przenośne, które będą służyły do wynoszenia informacji poza obręb pomieszczenia powinny być wyposażone w oprogramowanie lub rozwiązanie sprzętowe umożliwiające szyfrowanie danych z użyciem hasła dostępowego nie krótszego niż 8 znaków (hasło złożone co najmniej 1 duża litera, 1 cyfra i znak specjalny).
- Rozmieszczenie sprzętu:
 - stacja robocza powinna być ustawiona w miejscu uniemożliwiającym do niej dostęp osobom nieupoważnionym,
 - zalecane jest takie ustawienie monitora, aby nie było możliwości podejrzenia danych wyświetlonych na ekranie przez osoby nieuprawnione oraz ustawienie czasu automatycznego uruchamiania wygaszacza ekranu na maksymalnie 10 minut. Wznowienie pracy powinno wymagać podania hasła. Zalecane jest także blokowanie stacji przy każdorazowym opuszczeniu stanowiska,
 - zalecane jest takie ustawienie drukarki, aby nie było możliwości podejrzenia bądź pobrania wydruków przez osoby nieuprawnione.
- Kopie bezpieczeństwa:

- zalecane jest wdrożenie procedury tworzenia kopii zapasowych zapewniające wykonywanie kopii nie rzadziej niż raz na 30 dni.

5.2.4.2. *Poziom zalecany*

- Zaleca się wprowadzenie w BIOS następujących ustawień:
 - wejście i zmiana ustawień BIOS wymaga podania hasła,
 - uruchomienie komputera wymaga podania hasła,
 - wyłączona możliwość uruchamiania systemu z sieci lub innych nośników niż dysk twardy komputera,
 - długość hasła BIOS wynosi nie mniej niż 8 znaków (co najmniej 1 duża litera i 1 cyfra).
- Konta użytkowników i hasła:
 - wbudowane konto administratora powinno być używane tylko w przypadku wykonywania czynności administratora,
 - każdemu użytkownikowi komputera powinno być założone oddzielne konto, konta te nie powinny mieć przypisanych uprawnień administratora,
 - długość nazwy użytkownika powinna wynosić nie mniej niż 6 znaków,
 - długość hasła konta administratora lub użytkownika z uprawnieniami administratora powinna wynosić nie mniej niż 12 (hasło złożone co najmniej 1 duża litera, 1 cyfra i znak specjalny), okres ważności hasła nie powinien być dłuższy niż 30 dni,
 - długość hasła konta użytkownika powinna wynosić nie mniej niż 8 (hasło złożone co najmniej 1 duża litera, 1 cyfra i znak specjalny), okres ważności hasła nie powinien być dłuższy niż 30 dni,
 - zaleca się wprowadzić regulacje sankcjonujące zmianę pin-kodu mikroprocesorowych kart kryptograficznych nie rzadziej niż co 30 dni,
 - zalecane jest zastąpienie logowania tradycyjnego (login i hasło) logowaniem z użyciem kart mikroprocesorowych, czytników cech biometrycznych, kluczy bezprzewodowych,
 - zaleca się wprowadzić stosowne regulacje sankcjonujące sposoby przechowywania nazw użytkowników i haseł oraz zabraniające udostępnia ich innym osobom.
- Ochrona przed atakami zewnętrznymi (zapora ogniowa):
 - zaleca się zastosowanie 2 zapór ogniowych – sprzętowej na styku z siecią Internet oraz programowej na stacji roboczej, oraz wdrożenie regulacji zapewniających ich bieżącą aktualizację.
- Sieci Wi-Fi:
 - do połączenia z sieciami Wi-Fi zaleca się używać co najmniej standardu WPA i haseł o długości nie mniejszej niż 12 znaków (hasło złożone co najmniej 1 duża litera, 1 cyfra i znak specjalny).
- Ochrona antywirusowa:
 - zaleca się aby oprogramowanie antywirusowe instalowane na stacjach przetwarzających dane osobowe miało włączoną ochronę w czasie rzeczywistym,
 - zaleca się konfigurację oprogramowania zapewniającą bieżącą aktualizację sygnatur antywirusowych,
 - zaleca się konfigurację oprogramowania zapewniającą pełne skanowanie antywirusowe stacji co najmniej 1 raz w tygodniu.
- Aktualizacja Systemu i oprogramowania:

- zalecane jest stosowanie systemów operacyjnych wyłącznie w wersjach wspieranych przez ich producentów,
- zalecane jest włączenie automatycznych aktualizacji systemu oraz oprogramowania zgodnie z zaleceniami producentów.
- Usuwanie danych:
 - zaleca się konfigurację „kosza” systemowego, aby nie przechowywał usuniętych plików,
 - zaleca się do usuwania danych używać dedykowanego do tego celu oprogramowania.
- Dyski i urządzenia przenośne:
 - w przypadku stosowania dysków twardych umieszczonych w wymiowych kieszeniach powinny być one wyposażone w zamknięcie na kluczyk i zamknięte gdy znajduje się w nich dysk. Po zakończonej pracy zaleca się usunąć dysk i przechowywać w zabezpieczonej szafie,
 - zaleca się wdrożyć regulacje (w tym ewidencję nośników) zapewniające obsługę pamięci flash, oraz dysków przenośnych, podłączanych okresowo do stacji, zawierających dane, tak aby po zakończeniu pracy były one usuwane ze stacji i przechowywane w bezpieczny sposób,
 - przenośne pamięci flash oraz dyski przenośne które będą służyły do wynoszenia informacji poza obręb pomieszczenia powinny być wyposażone w rozwiązanie sprzętowe umożliwiające szyfrowanie danych z użyciem hasła dostępowego nie krótszego niż 8 znaków (hasło złożone co najmniej 1 duża litera, 1 cyfra i znak specjalny) lub w czytnik identyfikacji biometrycznej.
- Rozmieszczenie sprzętu:
 - stacja robocza powinna być ustawiona w miejscu uniemożliwiającym do niej dostęp osobom nieupoważnionym,
 - zalecane jest takie ustawienie monitora, aby nie było możliwości podejrzenia danych wyświetlonych na ekranie przez osoby nieuprawnione oraz ustawienie czasu automatycznego uruchamiania wygaszacza ekranu na maksymalnie 5 minut. Wznowienie pracy powinno wymagać podania hasła. Zalecane jest także blokowanie stacji przy każdorazowym opuszczeniu stanowiska,
 - zalecane jest takie ustawienie drukarki aby nie było możliwości podejrzenia bądź pobrania wydruków przez osoby nieuprawnione.
- Kopie bezpieczeństwa:
 - zalecane jest wdrożenie procedury tworzenia kopii zapasowych zapewniające wykonywanie kopii nie rzadziej niż raz na 7 dni,
 - składowanie kopii zapasowych powinno odbywać się w innym budynku bądź pomieszczeniach w odpowiednio zabezpieczonej szafie.
- Zasilanie awaryjne:
 - stacje robocze powinny być wyposażone w urządzenia podtrzymujące zasilanie (UPS) umożliwiające automatyczne bezpieczne zakończenie pracy w przypadku utraty zasilania podstawowego.

5.2.5. Środowiska wirtualne (maszyny wirtualne)

5.2.5.1. *Poziom minimalny*

- Zabezpieczenia serwerów/stacji udostępniających maszyny wirtualne oraz zabezpieczenia systemu udostępnianego z wykorzystaniem maszyny wirtualnej powinny być co najmniej na poziomie minimalnym opisanym w rozdziale 5.2.4.1.
- Uprawnienia do katalogu oraz dostęp do folderu udostępnianego powinny zostać ograniczone tylko do użytkowników maszyny wirtualnej.
- Uprawnienia do katalogu oraz dostęp do folderu udostępnianego powinien uniemożliwiać skopiowanie pliku maszyny przez osobę inną niż Administrator.
- Stosowanie maszyn wirtualnych na dyskach przenośnych bądź pamięciach typu flash nie jest zalecane. W przypadku konieczności stosowania rozwiązania zaleca się, aby:
 - nośnik plików maszyny wirtualnej był w całości zaszyfrowany,
 - wdrożyć regulacje zapewniające prawidłowe posługiwanie się nośnikami oraz prowadzić ewidencję dysków przenośnych bądź pamięci flash,
 - nośniki nie powinny być wynoszone poza obszar przetwarzania danych osobowych lub muszą być wyposażone w rozwiązanie umożliwiające szyfrowanie danych z użyciem hasła dostępowego nie krótszego niż 8 znaków (hasło złożone co najmniej 1 duża litera, 1 cyfra i znak specjalny) uniemożliwiające skorzystanie z danych po max 5 próbach nieudanego podania hasła do odblokowania nośnika.

5.2.5.2. *Poziom zalecany*

- Zabezpieczenia serwerów udostępniających maszyny wirtualne oraz zabezpieczenia systemu udostępnianego z wykorzystaniem maszyny wirtualnej są na poziomie nie mniejszym niż podstawowym opisanym w rozdziale 5.2.4.2.
- Uprawnienia do katalogu oraz dostęp do folderu udostępnianego powinny zostać ograniczone tylko do użytkowników maszyny wirtualnej.
- Uprawnienia do katalogu oraz dostęp do folderu udostępnianego powinien uniemożliwiać skopiowanie pliku maszyny przez osobę inną niż Administrator.
- Stosowanie maszyn wirtualnych na dyskach przenośnych bądź pamięciach typu flash nie jest zalecane. W przypadku konieczności stosowania rozwiązania zaleca się, aby:
 - nośnik plików maszyny wirtualnej był w całości zaszyfrowany,
 - wdrożyć regulacje zapewniające prawidłowe posługiwanie się nośnikami oraz prowadzić ewidencję dysków przenośnych bądź pamięci flash,
 - nośniki nie powinny być wynoszone poza obszar przetwarzania danych osobowych lub muszą być wyposażone w rozwiązanie umożliwiające szyfrowanie danych z użyciem hasła dostępowego nie krótszego niż 10 znaków (hasło złożone co najmniej 1 duża litera, 1 cyfra i znak specjalny) uniemożliwiające skorzystanie z danych po max 3 próbach nieudanego podania hasła do odblokowania nośnika.

5.2.6. Sprzęt komputerowy przenośny (laptop, tablet, itp.)

5.2.6.1. *Zalecenia minimalne*

- Wprowadzenie w BIOS ustawień opisanych w rozdziale 5.2.4.1.
- Zastosowanie konfiguracji Kont użytkowników i haseł opisanej w rozdziale 5.2.4.1.

- Ochrona przed atakami zewnętrznymi (zapora ogniowa) zgodnie z opisem w rozdziale 5.2.4.1.
- Sieci Wi-Fi:
 - do połączenia z sieciami Wi-Fi zaleca się używać co najmniej standardu WPA i haseł o długości nie mniejszej niż 12 znaków (hasło złożone co najmniej 1 duża litera, 1 cyfra i znak specjalny).
- Ochrona antywirusowa skonfigurowana zgodnie z opisem w rozdziale 5.2.4.1.
- Aktualizacja Systemu i oprogramowania zastosowane zgodnie z opisem w rozdziale 5.2.4.1.
- Zaleca się wykonywać usuwanie danych zgodnie z opisem w rozdziale 5.2.4.1.
- Dyski i urządzenia przenośne skonfigurowane zgodnie z opisem w rozdziale 5.2.4.1.
- Rozmieszczenie sprzętu:
 - stacja przenośna powinna być użytkowana w sposób uniemożliwiający do niej dostęp osobom nieupoważnionym,
 - stacje przenośną w miejscach korzystania powinno się zabezpieczyć linką antykradzieżową przymocowaną do stałego elementu wyposażenia (o ile jest to możliwe),
 - zaleca się ustawienie czasu automatycznego uruchamiania wygaszacza ekranu na maksymalnym poziomie 5 minut, wznowienie pracy wymaga podania hasła, blokowanie stacji przy każdorazowym opuszczeniu stanowiska,
 - w przypadku stosowania drukarki przenośnej wymagane jest takie ustawienie drukarki aby nie było możliwości podejrzenia bądź pobrania wydruków przez osoby nieuprawnione.
- Zaleca się wykonywanie kopii bezpieczeństwa zgodnie z opisem w rozdziale 5.2.4.1.
- Zasilanie awaryjne:
 - Stan baterii stacji przenośnej musi umożliwiać bezpieczne zamknięcie systemu po zaniku zasilania sieciowego.

5.2.6.2. *Zalecenia podstawowe*

- Wprowadzenie w BIOS ustawień opisanych w rozdziale 5.2.4.2.
 - Dodatkowo zaleca się używanie do logowania kart mikroprocesorowych bądź czytników biometrycznych (o ile jest taka możliwość).
- Zastosowanie konfiguracji Kont użytkowników i haseł opisanej w rozdziale 5.2.4.2.
- Ochrona przed atakami zewnętrznymi (zapora ogniowa) zgodnie z opisem w rozdziale 5.2.4.2.
- Sieci Wi-Fi:
 - do połączenia z sieciami Wi-Fi zaleca się używać co najmniej standardu WPA2 i haseł o długości nie mniejszej niż 14 znaków (hasło złożone co najmniej 1 duża litera, 1 cyfra i znak specjalny).
- Ochrona antywirusowa skonfigurowana zgodnie z opisem w rozdziale 5.2.4.2.
- Aktualizacja Systemu i oprogramowania zastosowane zgodnie z opisem w rozdziale 5.2.4.2.
- Zaleca się wykonywać usuwanie danych zgodnie z opisem w rozdziale 5.2.4.2.
- Dyski i urządzenia przenośne skonfigurowane zgodnie z opisem w rozdziale 5.2.4.2.
 - Dodatkowo partycja lub dysk stacji przenośnej na której są składowane dane jest w całości zaszyfrowany przy wykorzystaniu sprzętowego modułu szyfrowania lub programowo, przy użyciu algorytmu AES256.

- Rozmieszczenie sprzętu:
 - stacja przenośna powinna być użytkowana w sposób uniemożliwiający do niej dostęp osobom nieupoważnionym,
 - stacje przenośną w miejscach korzystania powinno się zabezpieczyć linką antykradzieżową przymocowaną do stałego elementu wyposażenia (o ile jest to możliwe),
 - zaleca się ustawienie czasu automatycznego uruchamiania wygaszacza ekranu na maksymalnym poziomie 5 minut, wznowienie pracy wymaga podania hasła, blokowanie stacji przy każdorazowym opuszczeniu stanowiska,
 - w przypadku stosowania drukarki przenośnej wymagane jest takie ustawienie drukarki aby nie było możliwości podejrzenia bądź pobrania wydruków przez osoby nieuprawnione.
- Zaleca się wykonywanie kopii bezpieczeństwa zgodnie z opisem w rozdziale 5.2.4.2.
- Zasilanie awaryjne:
 - Stan baterii powinien umożliwiać bezpieczne zamknięcie systemu po zaniku zasilania sieciowego.

6. Użytkownicy Indywidualni

Niniejszy rozdział dotyczy Użytkowników Indywidualnych, którzy korzystają z aplikacji przeglądarkowych (cienki klient) udostępnianych przez system CEPiK 2.0.

6.1. Dokumentacja opisująca sposób przetwarzania danych osobowych

Każdy Użytkownik Indywidualny systemu CEPiK 2.0 z chwilą pozyskania danych osobowych z systemu CEPiK staje się administratorem tych danych. Zgodnie z art. 36 ust 1 *ustawy o ochronie danych osobowych* administrator danych obowiązany zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabranieniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem. Zgodnie z art. 36 ust 2 tej ustawy administrator danych prowadzi dokumentację opisującą sposób przetwarzania danych oraz środki wskazane w zdaniu poprzednim.

Zgodnie z § 3 ust. 1 *rozporządzenia Ministra Spraw Wewnętrznych i Administracji w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych*, na dokumentację, o której mowa w poprzednim akapicie, składa się polityka bezpieczeństwa i instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

Polityka bezpieczeństwa zawiera w szczególności (zgodnie z § 4 ww. rozporządzenia):

1. wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe,
2. wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych,
3. opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi,
4. sposób przepływu danych pomiędzy systemami,
5. środki techniczne i organizacyjne niezbędne do zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.

Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych zawiera w szczególności (zgodnie z § 5 ww. rozporządzenia):

1. procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za tę czynność,
2. stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem,
3. procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu,
4. procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania,
5. sposób, miejsce i okres przechowywania:
6. elektronicznych nośników informacji zawierających dane osobowe,

7. kopii zapasowych, o których mowa w pkt 4,
8. sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego,
9. sposób realizacji wymogów w zakresie odnotowywania informacji związanych z przetwarzaniem danych osobowych takich jak: data wprowadzenia danych, identyfikator użytkownika wprowadzającego dane, źródła danych, informacji o odbiorcach danych, w tym dacie i zakresie udostępnionych danych,
10. procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych.

Każdy Użytkownik Instytucjonalny, z chwilą podłączenia do systemu CEPiK 2.0, zobowiązany jest do posiadania wskazanej powyżej dokumentacji.

6.2.Środki ochrony kryptograficznej

W systemie CEPiK 2.0 stosowane są środki kryptograficznej ochrony danych. Każdy Użytkownik Indywidualny musi posiadać odpowiedni certyfikat, aby móc skorzystać z usług systemu CEPiK 2.0. Szczegółowy sposób uzyskania certyfikatów, ich wymiany, sposób ochrony kluczy prywatnych oraz inne informacje i wymagania związane z certyfikatami są opisane w dokumentach:

- Polityka certyfikacji dla infrastruktury systemu informatycznego CEPiK 2.0;
- Polityka certyfikacji dla operatorów systemu informatycznego CEPiK 2.0.

W ramach polityki certyfikacji dla infrastruktury systemu informatycznego CEPiK 2.0 wydawane są certyfikaty dla systemów zewnętrznych służące do autoryzacji, uwierzytelniania, podpisywania komunikatów i zestawiania SSL (certyfikaty SSL), oraz certyfikaty służące do zestawiania połączeń VPN (certyfikaty VPN).

W ramach polityki certyfikacji dla operatorów systemu informatycznego CEPiK 2.0 wydawane są certyfikaty dla użytkowników aplikacji przeglądarkowych udostępnianych przez system CEPiK 2.0 służące do autoryzacji, uwierzytelniania, podpisywania komunikatów i zestawiania SSL (certyfikaty SSL).

6.3.Połączenie z systemem CEPiK 2.0

Użytkownik Indywidualny ma możliwość połączenia się z systemem CEPiK 2.0 przez sieć publiczną Internet oraz przez sieć wydzieloną np. OST112, GovNet, sTesta, PESEL-NET.

Użytkownik Indywidualny łączący się z systemem CEPiK 2.0 przez sieć publiczną Internet musi zestawić bezpieczne połączenie VPN z wykorzystaniem certyfikatu VPN. Dopiero po zestawieniu połączenia VPN użytkownik ma możliwość wywołania w przeglądarce internetowej aplikacji systemu CEPiK 2.0. Autoryzacja i uwierzytelnienie Użytkownika w aplikacjach systemu CEPiK 2.0 są realizowane w oparciu o posiadany przez Użytkownika certyfikat SSL umieszczony na mikroprocesorowej karcie kryptograficznej.

Użytkownik Indywidualny łączący się z systemem CEPiK 2.0 przez sieć wydzieloną ma możliwość wywołania aplikacji systemu CEPiK 2.0 bez konieczności zestawiania bezpiecznego połączenia VPN – autoryzacja i uwierzytelnienie Użytkownika w aplikacjach systemu CEPiK 2.0 są realizowane w

oparciu o posiadany przez Użytkownika certyfikat SSL umieszczony na mikroprocesorowej karcie kryptograficznej.

System CEPiK 2.0 wspiera rozwiązania programowe Cisco VPN Client oraz Cisco AnyConnect i komunikację VPN typu Remote Access. Dla tych rozwiązań Service Desk zapewni wsparcie związane z instalacją oraz konfiguracją oprogramowania. Rozwiązanie VPN typu Remote Access będzie wymuszało politykę bezpieczeństwa sieci, m.in. po zestawieniu połączenia VPN dostęp do zasobów sieci publicznej Internet będzie ograniczony, możliwe będzie wywoływanie usług CEPiK 2.0.

System CEPiK 2.0 dopuszcza połączenia VPN typu Lan-to-Lan, przy czym ich nie wspiera. Każdy Użytkownik Indywidualny decydujący się na takie połączenie powinien je zestawić we własnym zakresie, na podstawie wskazanych do zastosowania parametrów konfiguracyjnych. Przed implementacją takiego rozwiązania należy skontaktować się z Service Desk CEPiK w celu otrzymania niezbędnych danych i informacji, które umożliwią konfigurację urządzeń po stronie użytkownika.

6.4.Rozliczalność

System CEPiK 2.0 zapewnia pełną rozliczalność działań Użytkowników Indywidualnych w systemie, w szczególności w zakresie operacji wykonywanych na danych osobowych. Każde działanie użytkownika podlega odnotowaniu w podsystemie logowania CEPiK 2.0. Użytkownik jest identyfikowany w oparciu o spersonalizowany certyfikat SSL, który jest wydawany dla konkretnej osoby i zawiera jednoznacznie identyfikujące daną osobę informacje.

6.5.Podpisywanie komunikatów

Podpisywanie komunikatów przekazywanych do systemu CEPiK 2.0 przez aplikacje przeglądarkowe systemu CEPiK 2.0 zapewnia dana aplikacja.

7. Zalecenia i wytyczne dla Użytkowników Indywidualnych w zakresie ochrony danych osobowych

7.1.Ochrona fizyczna

Niniejszy rozdział opisuje zalecenia w zakresie ochrony fizycznej pomieszczeń, w których będą przetwarzane dane osobowe, oraz ochrony fizycznej urządzeń wykorzystywanych do przetwarzania danych osobowych, które będą zlokalizowane w tych pomieszczeniach.

7.1.1. Pomieszczenia i ich lokalizacja

7.1.1.1. Poziom minimalny

- Pomieszczenia, w których będą przetwarzane dane osobowe, powinny zapewniać takie rozmieszczenie urządzeń oraz dokumentów, aby uniemożliwić dostęp (m.in. wgląd, podejrzenie) do danych osobowych osobom nieuprawnionym do dostępu do tych danych, np. przez zastosowanie wygradzeń, żaluzji, odpowiednie ustawienie monitora względem okna i drzwi.
- Pomieszczenia, w których będą przetwarzane dane osobowe, powinny być zlokalizowane w miejscach gdzie ryzyko ich zatopienia lub zalania jest zminimalizowane.

7.1.1.2. Poziom zalecany

- Pomieszczenia, w których będą przetwarzane dane osobowe, powinny zapewniać takie rozmieszczenie urządzeń oraz dokumentów, aby uniemożliwić dostęp (m.in. wgląd, podejrzenie) do danych osobowych osobom nieupoważnionym do dostępu do tych danych, np. przez zastosowanie wygradzeń, żaluzji, odpowiednie ustawienie monitora względem okna i drzwi.
- Pomieszczenia, w których będą przetwarzane dane osobowe, nie powinny być pomieszczeniami przechodnimi.
- Pomieszczenia, w których będą przetwarzane dane osobowe, powinny być wyposażone w system alarmowy, system przeciwpożarowy, np. czujniki zadymienia wraz z funkcją powiadomienia do służby ochrony lub jednostek straży pożarnej, policji.

7.1.2. Kontrola dostępu do pomieszczeń

7.1.2.1. Poziom minimalny

- Zaleca się w przypadku braku systemu elektronicznej kontroli dostępu, wdrożenie manualnej kontroli dostępu do pomieszczeń, w których będą przetwarzane dane osobowe, w sposób organizacyjny – proceduralny, np. książka pobrań kluczy.
- Dostęp do pomieszczeń, w których będą przetwarzane dane osobowe, powinny posiadać wyłącznie osoby uprawnione.
- Jeżeli istnieje taka konieczność, inne osoby mogą przebywać w tych pomieszczeniach jedynie w obecności osób uprawnionych, za ich wiedzą i zgodą.

7.1.2.2. Poziom zalecany

- Zaleca się zastosowanie systemu elektronicznej kontroli dostępu do pomieszczeń, w których będą przetwarzane dane osobowe.
- Urządzenia automatycznej kontroli dostępu winny być nadzorowane całodobowo przez służbę ochrony.
- Zaleca się wdrożenie procedury cyklicznego sprawdzenia logów systemu elektronicznej kontroli dostępu do pomieszczeń.
- Dostęp do pomieszczeń powinny posiadać wyłącznie osoby uprawnione.
- Jeżeli istnieje taka konieczność, inne osoby mogą przebywać w tych pomieszczeniach jedynie w obecności osób uprawnionych, za ich wiedzą i zgodą.
- Zaleca się stosowanie systemu elektronicznej kontroli dostępu do pomieszczeń w celu odnotowania wejść osób nieuprawnionych lub zastosowanie środków organizacyjno – proceduralnych, np. odnotowywanie wejść osób nieuprawnionych w książce wejść.

7.1.3. Zabezpieczenie drzwi i okien

7.1.3.1. Poziom minimalny

- Drzwi do pomieszczeń, w których będą przetwarzane dane osobowe, powinny być zabezpieczone przed wyważeniem (podważeniem) oraz wyposażone w bezpieczny zamek.
- Otwory okienne pomieszczeń zlokalizowanych na parterze lub ostatniej kondygnacji (o ile jest swobodny dostęp do dachu) powinny być okratowane lub zabezpieczone w inny, równoważny sposób (np. folią antywłamaniową).

7.1.3.2. Poziom zalecany

- Drzwi do pomieszczeń, w których będą przetwarzane dane osobowe, znajdujących się wewnątrz budynku w strefie ograniczonego dostępu (bądź strefie dozorowanej) powinny być zabezpieczone przed wyważeniem i wyposażone w co najmniej 1 zamek atestowany (klasa C).
- Drzwi znajdujące się wewnątrz budynku w strefie ogólnodostępnej niedozorowanej powinny spełniać wymagania co najmniej klasy 2 zgodnie z normą PN-EN14351-1+A1:2010 oraz być wyposażone w co najmniej jeden zamek atestowany (klasa C).
- Drzwi, do których dostęp jest z zewnątrz budynku, powinny spełniać wymagania co najmniej klasy 3 zgodnie z normą PN-EN14351-1+A1:2010.
- Otwory okienne pomieszczeń zlokalizowanych na parterze lub ostatniej kondygnacji (o ile jest swobodny dostęp do dachu) powinny być okratowane lub posiadać okna spełniające wymagania co najmniej klasy 2 zgodnie z normą PN-EN14351-1+A1:2010 z szybą klasy P4.

7.2. Zabezpieczenia urządzeń oraz nośników danych

7.2.1. Nośniki danych i informacji

7.2.1.1. Poziom minimalny

- Dokumenty i nośniki informacji zawierające dane osobowe powinny być przechowywane w miejscu uniemożliwiającym dostęp do nich osobom nieupoważnionym (np. w zamykanych na klucz szafkach).
- Do likwidacji wydruków dokumentów i nośników informacji powinno się stosować przeznaczony do tego celu niszczarkę.

7.2.1.2. Poziom zalecany

- Dane przechowywane na elektronicznych oraz papierowych nośnikach danych powinny być składowane w szafach wyposażonych w co najmniej 1 zamek atestowany (klasa A).
- Do likwidacji wydruków dokumentów i nośników informacji powinno się stosować niszczarkę klasy DIN 3 zgodnie z normą DIN 32757.

7.2.2. Urządzenia służące do nawiązywania komunikacji za pomocą sieci dedykowanych

7.2.2.1. Zalecenia w zakresie konfiguracji urządzeń

- Użytkownicy łączący się z systemem CEPiK poprzez sieci dedykowane powinni stosować się do wymagań i zaleceń określonych dla konkretnej sieci dedykowanej.
- Urządzenia sieciowe (takie jak routery oraz przełączniki sieciowe) pozwalające na dostęp do sieci dedykowanej powinny być zabezpieczone przed nieuprawnionym dostępem osób trzecich:
 - Administracja zdalna powinna być odpowiednio zabezpieczona przed nieuprawnionym dostępem za pomocą mechanizmów uwierzytelnienia routera (np. login i hasło o odpowiedniej złożoności).
 - Administracja zdalna powinna być uruchomiona wyłącznie na jednym porcie wewnętrznym, do którego ma dostęp wyłącznie administrator danego urządzenia.
 - Powinna być wdrożona reglamentacja dostępu do sieci np. na podstawie adresów MAC.

7.2.2.2. *Zalecenia w zakresie bezpieczeństwa fizycznego urządzeń*

- Urządzenia sieciowe powinny być zlokalizowane w pomieszczeniu lub szafie z ograniczonym dostępem osób trzecich. Dostęp do tego pomieszczenia lub szafy powinien mieć wyłącznie administrator urządzenia lub osoby upoważnione.

7.2.3. Urządzenia i oprogramowanie służące do nawiązania połączeń VPN przez sieć publiczną Internet

7.2.3.1. *Zalecenia w zakresie konfiguracji urządzeń i oprogramowania*

- Użytkownicy łączący się z systemem CEPiK poprzez sieć publiczną Internet, aby uzyskać dostęp do systemu CEPiK, muszą zestawić bezpieczne połączenie VPN z wykorzystaniem certyfikatu.
- Urządzenia sieciowe (takie jak routery) pozwalające na zestawienie połączeń VPN powinny być zabezpieczone przed nieuprawnionym dostępem osób trzecich:
 - Urządzenie powinno być zabezpieczone w sposób uniemożliwiający osobom nieuprawnionym pozyskanie kluczy prywatnych do certyfikatu VPN, zainstalowanych w urządzeniu.
 - Administracja zdalna powinna być odpowiednio zabezpieczona przed nieuprawnionym dostępem za pomocą mechanizmów uwierzytelnienia routera (np. login i hasło o odpowiedniej złożoności).
 - Administracja zdalna powinna być uruchomiona wyłącznie na jednym porcie wewnętrznym, do którego ma dostęp wyłącznie administrator danego urządzenia.
- Powinna być wdrożona reglamentacja dostępu do sieci np. na podstawie adresów MAC.
- Powinna być wdrożona polityka blokowania dostępu do i z sieci publicznej Internet w czasie, w którym jest nawiązywane połączenie VPN.
- Oprogramowanie służące do zestawiania połączeń VPN (typu Remote Access) powinno być zabezpieczone w taki sposób, aby uniemożliwić dostęp do kluczy prywatnych osobom nieuprawnionym.
- Oprogramowanie służące do zestawiania połączeń VPN (typu Remote Access) powinno wymuszać blokowanie dostępu do i z sieci publicznej Internet do danej stacji komputerowej w czasie, w którym jest nawiązywane połączenie VPN (jest to wymuszone przez konfigurację urządzeń po stronie systemu CEPiK).

7.2.3.2. *Zalecenia w zakresie bezpieczeństwa fizycznego urządzeń*

- Urządzenia sieciowe powinny być zlokalizowane w pomieszczeniu lub szafie z ograniczonym dostępem osób trzecich. Dostęp do tego pomieszczenia lub szafy powinien mieć wyłącznie administrator urządzenia lub osoby upoważnione.

7.2.4. Sprzęt komputerowy stacjonarny

7.2.4.1. *Poziom minimalny*

- Zaleca się wprowadzenie w BIOS następujących ustawień:
 - wejście i zmiana ustawień BIOS wymaga podania hasła,
 - wyłączona jest możliwość uruchamiania systemu z sieci lub innych nośników niż dysk twardy komputera,
 - długość hasła BIOS powinna wynosić nie mniej niż 6 znaków (co najmniej 1 duża litera i 1 cyfra).

- Konta użytkowników i hasła:
 - wbudowane konto administratora powinno być używane tylko w przypadku wykonywania czynności administratora,
 - każdemu użytkownikowi komputera powinno być założone oddzielne konto, konta te nie powinny mieć przypisanych uprawnień administratora, o ile nie jest to wymagane do bieżącej pracy,
 - długość nazwy użytkownika powinna wynosić nie mniej niż 3 znaki,
 - długość hasła konta administratora lub użytkownika z uprawnieniami administratora powinna wynosić nie mniej niż 10 znaków (hasło złożone co najmniej 1 duża litera, 1 cyfra i znak specjalny), okres ważności hasła nie powinien być dłuższy niż 30 dni,
 - długość hasła konta użytkownika powinna wynosić nie mniej niż 8 znaków (hasło złożone co najmniej 1 duża litera, 1 cyfra i znak specjalny), okres ważności hasła nie dłuższy niż 30 dni,
 - zaleca się wprowadzić regulacje sankcjonujące zmianę pin-kodu mikroprocesorowych kart kryptograficznych nie rzadziej niż co 30 dni,
 - zaleca się wprowadzić stosowne regulacje sankcjonujące sposoby przechowywania nazw użytkowników i haseł oraz zabraniające udostępnia ich innym osobom.
- Ochrona przed atakami zewnętrznymi (zapora ogniowa):
 - zalecane jest zastosowanie zapory ogniowej (sprzętowej lub programowej) oraz wdrożenie regulacji zapewniających jej bieżącą aktualizację.
- Sieci Wi-Fi:
 - do połączenia z sieciami Wi-Fi zaleca się używać co najmniej standardu WPA i haseł o długości nie mniejszej niż 12 znaków (hasło złożone co najmniej 1 duża litera, 1 cyfra i znak specjalny).
- Ochrona antywirusowa:
 - zalecane jest zainstalowanie oprogramowania antywirusowego oraz wdrożenie regulacji zapewniających aktualizację sygnatur antywirusowych nie rzadziej niż raz w tygodniu,
 - zalecane jest wdrożenie regulacji zapewniających pełne skanowanie antywirusowe stacji co najmniej 1 raz w tygodniu w przypadku braku ochrony w czasie rzeczywistym i nie mniej niż 1 raz w miesiącu w przypadku stosowania ochrony w czasie rzeczywistym.
- Aktualizacja systemu i oprogramowania:
 - zalecane jest stosowanie systemów operacyjnych w wersjach wspieranych przez ich producentów,
 - zalecane jest wdrożenie regulacji związanych z aktualizowaniem systemu operacyjnego oraz wykorzystywanego oprogramowania zgodnie z zaleceniami producentów.
- Usuwanie danych:
 - zaleca się konfigurację „kosza” systemowego, aby nie przechowywał usuniętych plików.
- Dyski i urządzenia przenośne:
 - w przypadku stosowania dysków twardych umieszczonych w wyjmowanych kieszeniach powinny być one wyposażone w zamknięcie na klucz i zamknięte, gdy

znajduje się w nich dysk. Po zakończonej pracy zalecane jest usunięcie dysku i jego dalsze przechowywanie w zabezpieczonej szafie,

- powinny być wdrożone regulacje zapewniające obsługę pamięci flash, oraz dysków przenośnych, podłączanych okresowo do stacji, zawierających dane, tak aby po zakończeniu pracy były one usuwane ze stacji i przechowywać w bezpieczny sposób,
- przenośne pamięci flash oraz dyski przenośne, które będą służyły do wynoszenia informacji poza obręb pomieszczenia powinny być wyposażone w oprogramowanie lub rozwiązanie sprzętowe umożliwiające szyfrowanie danych z użyciem hasła dostępowego nie krótszego niż 8 znaków (hasło złożone co najmniej 1 duża litera, 1 cyfra i znak specjalny).
- Rozmieszczenie sprzętu:
 - stacja robocza powinna być ustawiona w miejscu uniemożliwiającym do niej dostęp osobom nieupoważnionym,
 - zalecane jest takie ustawienie monitora, aby nie było możliwości podejrzenia danych wyświetlonych na ekranie przez osoby nieuprawnione oraz ustawienie czasu automatycznego uruchamiania wygaszacza ekranu na maksymalnie 10 minut. Wznowienie pracy powinno wymagać podania hasła. Zalecane jest także blokowanie stacji przy każdorazowym opuszczeniu stanowiska,
 - zalecane jest takie ustawienie drukarki, aby nie było możliwości podejrzenia bądź pobrania wydruków przez osoby nieuprawnione.
- Kopie bezpieczeństwa:
 - zalecane jest wdrożenie procedury tworzenia kopii zapasowych zapewniające wykonywanie kopii nie rzadziej niż raz na 30 dni.

7.2.4.2. Poziom zalecany

- Zaleca się wprowadzenie w BIOS następujących ustawień:
 - wejście i zmiana ustawień BIOS wymaga podania hasła,
 - uruchomienie komputera wymaga podania hasła,
 - wyłączona możliwość uruchamiania systemu z sieci lub innych nośników niż dysk twardy komputera,
 - długość hasła BIOS wynosi nie mniej niż 8 znaków (co najmniej 1 duża litera i 1 cyfra).
- Konta użytkowników i hasła:
 - wbudowane konto administratora powinno być używane tylko w przypadku wykonywania czynności administratora,
 - każdemu użytkownikowi komputera powinno być założone oddzielne konto, konta te nie powinny mieć przypisanych uprawnień administratora,
 - długość nazwy użytkownika powinna wynosić nie mniej niż 6 znaków,
 - długość hasła konta administratora lub użytkownika z uprawnieniami administratora powinna wynosić nie mniej niż 12 (hasło złożone co najmniej 1 duża litera, 1 cyfra i znak specjalny), okres ważności hasła nie powinien być dłuższy niż 30 dni,
 - długość hasła konta użytkownika powinna wynosić nie mniej niż 8 (hasło złożone co najmniej 1 duża litera, 1 cyfra i znak specjalny), okres ważności hasła nie powinien być dłuższy niż 30 dni,
 - zaleca się wprowadzić regulacje sankcjonujące zmianę pin-kodu mikroprocesorowych kart kryptograficznych nie rzadziej niż co 30 dni,

- zalecane jest zastąpienie logowania tradycyjnego (login i hasło) logowaniem z użyciem kart mikroprocesorowych, czytników cech biometrycznych, kluczy bezprzewodowych,
 - zaleca się wprowadzić stosowne regulacje sankcjonujące sposoby przechowywania nazw użytkowników i haseł oraz zabraniające udostępnia ich innym osobom.
- Ochrona przed atakami zewnętrznymi (zapora ogniowa):
 - zaleca się zastosowanie 2 zapór ogniowych – sprzętowej na styku z siecią Internet oraz programowej na stacji roboczej, oraz wdrożenie regulacji zapewniających ich bieżącą aktualizację.
- Sieci Wi-Fi:
 - do połączenia z sieciami Wi-Fi zaleca się używać co najmniej standardu WPA i haseł o długości nie mniejszej niż 12 znaków (hasło złożone co najmniej 1 duża litera, 1 cyfra i znak specjalny).
- Ochrona antywirusowa:
 - zaleca się aby oprogramowanie antywirusowe instalowane na stacjach przetwarzających dane osobowe miało włączoną ochronę w czasie rzeczywistym,
 - zaleca się konfigurację oprogramowania zapewniającą bieżącą aktualizację sygnatur antywirusowych,
 - zaleca się konfigurację oprogramowania zapewniającą pełne skanowanie antywirusowe stacji co najmniej 1 raz w tygodniu.
- Aktualizacja Systemu i oprogramowania:
 - zalecane jest stosowanie systemów operacyjnych wyłącznie w wersjach wspieranych przez ich producentów,
 - zalecane jest włączenie automatycznych aktualizacji systemu oraz oprogramowania zgodnie z zaleceniami producentów.
- Usuwanie danych:
 - zaleca się konfigurację „kosza” systemowego, aby nie przechowywał usuniętych plików,
 - zaleca się do usuwania danych używać dedykowanego do tego celu oprogramowania.
- Dyski i urządzenia przenośne:
 - w przypadku stosowania dysków twardych umieszczonych w wyjmowanych kieszeniach powinny być one wyposażone w zamknięcie na kluczyk i zamknięte gdy znajduje się w nich dysk. Po zakończonej pracy zaleca się usunąć dysk i przechowywać w zabezpieczonej szafie,
 - zaleca się wdrożyć regulacje (w tym ewidencję nośników) zapewniające obsługę pamięci flash, oraz dysków przenośnych, podłączanych okresowo do stacji, zawierających dane, tak aby po zakończeniu pracy były one usuwane ze stacji i przechowywane w bezpieczny sposób,
 - przenośne pamięci flash oraz dyski przenośne które będą służyły do wynoszenia informacji poza obręb pomieszczenia powinny być wyposażone w rozwiązanie sprzętowe umożliwiające szyfrowanie danych z użyciem hasła dostępowego nie krótszego niż 8 znaków (hasło złożone co najmniej 1 duża litera, 1 cyfra i znak specjalny) lub w czytnik identyfikacji biometrycznej.
- Rozmieszczenie sprzętu:

- stacja robocza powinna być ustawiona w miejscu uniemożliwiającym do niej dostęp osobom nieupoważnionym,
- zalecane jest takie ustawienie monitora, aby nie było możliwości podejrzenia danych wyświetlonych na ekranie przez osoby nieuprawnione oraz ustawienie czasu automatycznego uruchamiania wygaszacza ekranu na maksymalnie 5 minut. Wznowienie pracy powinno wymagać podania hasła. Zalecane jest także blokowanie stacji przy każdorazowym opuszczeniu stanowiska,
- zalecane jest takie ustawienie drukarki aby nie było możliwości podejrzenia bądź pobrania wydruków przez osoby nieuprawnione.
- Kopie bezpieczeństwa:
 - zalecane jest wdrożenie procedury tworzenia kopii zapasowych zapewniające wykonywanie kopii nie rzadziej niż raz na 7 dni,
 - składowanie kopi zapasowych powinno odbywać się w innym budynku bądź pomieszczeniach w odpowiednio zabezpieczonej szafie.
- Zasilanie awaryjne:
 - stacje robocze powinny być wyposażone w urządzenia podtrzymujące zasilanie (UPS) umożliwiające automatyczne bezpieczne zakończenie pracy w przypadku utraty zasilania podstawowego.

7.2.5. Środowiska wirtualne (maszyny wirtualne)

7.2.5.1. *Poziom minimalny*

- Zabezpieczenia serwerów/stacji udostępniających maszyny wirtualne oraz zabezpieczenia systemu udostępnianego z wykorzystaniem maszyny wirtualnej powinny być co najmniej na poziomie minimalnym opisanym w rozdziale 7.2.4.1.
- Uprawnienia do katalogu oraz dostęp do folderu udostępnianego powinny zostać ograniczone tylko do użytkowników maszyny wirtualnej.
- Uprawnienia do katalogu oraz dostęp do folderu udostępnianego powinien uniemożliwiać skopiowanie pliku maszyny przez osobę inną niż Administrator.
- Stosowanie maszyn wirtualnych na dyskach przenośnych bądź pamięciach typu flash nie jest zalecane. W przypadku konieczności stosowania rozwiązania zaleca się, aby:
 - nośnik plików maszyny wirtualnej był w całości zaszyfrowany,
 - wdrożyć regulacje zapewniające prawidłowe posługiwanie się nośnikami oraz prowadzić ewidencję dysków przenośnych bądź pamięci flash,
 - nośniki nie powinny być wynoszone poza obszar przetwarzania danych osobowych lub muszą być wyposażone w rozwiązanie umożliwiające szyfrowanie danych z użyciem hasła dostępowego nie krótszego niż 8 znaków (hasło złożone co najmniej 1 duża litera, 1 cyfra i znak specjalny) uniemożliwiające skorzystanie z danych po max 5 próbach nieudanego podania hasła do odblokowania nośnika.

7.2.5.2. *Poziom zalecany*

- Zabezpieczenia serwerów udostępniających maszyny wirtualne oraz zabezpieczenia systemu udostępnianego z wykorzystaniem maszyny wirtualnej są na poziomie nie mniejszym niż podstawowym opisanym w rozdziałach 7.2.4.2.
- Uprawnienia do katalogu oraz dostęp do folderu udostępnianego powinny zostać ograniczone tylko do użytkowników maszyny wirtualnej.

- Uprawnienia do katalogu oraz dostęp do folderu udostępnianego powinien uniemożliwiać skopiowanie pliku maszyny przez osobę inną niż Administrator.
- Stosowanie maszyn wirtualnych na dyskach przenośnych bądź pamięciach typu flash nie jest zalecane. W przypadku konieczności stosowania rozwiązania zaleca się, aby:
 - nośnik plików maszyny wirtualnej był w całości zaszyfrowany,
 - wdrożyć regulacje zapewniające prawidłowe posługiwanie się nośnikami oraz prowadzić ewidencję dysków przenośnych bądź pamięci flash,
 - nośniki nie powinny być wynoszone poza obszar przetwarzania danych osobowych lub muszą być wyposażone w rozwiązanie umożliwiające szyfrowanie danych z użyciem hasła dostępowego nie krótszego niż 10 znaków (hasło złożone co najmniej 1 duża litera, 1 cyfra i znak specjalny) uniemożliwiające skorzystanie z danych po max 3 próbach nieudanego podania hasła do odblokowania nośnika.

7.2.6. Sprzęt komputerowy przenośny (laptop, tablet, itp.)

7.2.6.1. Poziom minimalny

- Wprowadzenie w BIOS ustawień opisanych w rozdziale 7.2.4.1.
- Zastosowanie konfiguracji Kont użytkowników i haseł opisanej w rozdziale 7.2.4.1.
- Ochrona przed atakami zewnętrznymi (zapora ogniowa) zgodnie z opisem w rozdziale 7.2.4.1.
- Sieci Wi-Fi:
 - do połączenia z sieciami Wi-Fi zaleca się używać co najmniej standardu WPA i haseł o długości nie mniejszej niż 12 znaków (hasło złożone co najmniej 1 duża litera, 1 cyfra i znak specjalny).
- Ochrona antywirusowa skonfigurowana zgodnie z opisem w rozdziale 7.2.4.1.
- Aktualizacja Systemu i oprogramowania zastosowane zgodnie z opisem w rozdziale 7.2.4.1.
- Zaleca się wykonywać usuwanie danych zgodnie z opisem w rozdziale 7.2.4.1.
- Dyski i urządzenia przenośne skonfigurowane zgodnie z opisem w rozdziale 7.2.4.1.
- Rozmieszczenie sprzętu:
 - stacja przenośna powinna być użytkowana w sposób uniemożliwiający do niej dostęp osobom nieupoważnionym,
 - stacje przenośną w miejscach korzystania powinno się zabezpieczyć linką antykradzieżową przymocowaną do stałego elementu wyposażenia (o ile jest to możliwe),
 - zaleca się ustawienie czasu automatycznego uruchamiania wygaszacza ekranu na maksymalnym poziomie 5 minut, wznowienie pracy wymaga podania hasła, blokowanie stacji przy każdorazowym opuszczeniu stanowiska,
 - w przypadku stosowania drukarki przenośnej wymagane jest takie ustawienie drukarki aby nie było możliwości podejrzenia bądź pobrania wydruków przez osoby nieuprawnione.
- Zaleca się wykonywanie kopii bezpieczeństwa zgodnie z opisem w rozdziale 7.2.4.1.
- Zasilanie awaryjne:
 - Stan baterii stacji przenośnej musi umożliwiać bezpieczne zamknięcie systemu po zaniku zasilania sieciowego.

7.2.6.2. *Poziom zalecany*

- Wprowadzenie w BIOS ustawień opisanych w rozdziale 7.2.4.2.
 - Dodatkowo zaleca się używanie do logowania kart mikroprocesorowych bądź czytników biometrycznych (o ile jest taka możliwość).
- Zastosowanie konfiguracji Kont użytkowników i haseł opisanej w rozdziale 7.2.4.2.
- Ochrona przed atakami zewnętrznymi (zapora ogniowa) zgodnie z opisem w rozdziale 7.2.4.2.
- Sieci Wi-Fi:
 - do połączenia z sieciami Wi-Fi zaleca się używać co najmniej standardu WPA2 i haseł o długości nie mniejszej niż 14 znaków (hasło złożone co najmniej 1 duża litera, 1 cyfra i znak specjalny).
- Ochrona antywirusowa skonfigurowana zgodnie z opisem w rozdziale 7.2.4.2.
- Aktualizacja Systemu i oprogramowania zastosowane zgodnie z opisem w rozdziale 7.2.4.2.
- Zaleca się wykonywać usuwanie danych zgodnie z opisem w rozdziale 7.2.4.2.
- Dyski i urządzenia przenośne skonfigurowane zgodnie z opisem w rozdziale 7.2.4.2.
 - Dodatkowo partycja lub dysk stacji przenośnej na której są składowane dane jest w całości zaszyfrowany przy wykorzystaniu sprzętowego modułu szyfrowania lub programowo, przy użyciu algorytmu AES256.
- Rozmieszczenie sprzętu:
 - stacja przenośna powinna być użytkowana w sposób uniemożliwiający do niej dostęp osobom nieupoważnionym,
 - stacje przenośną w miejscach korzystania powinno się zabezpieczyć linką antykradzieżową przymocowaną do stałego elementu wyposażenia (o ile jest to możliwe),
 - zaleca się ustawienie czasu automatycznego uruchamiania wygaszacza ekranu na maksymalnym poziomie 5 minut, wznowienie pracy wymaga podania hasła, blokowanie stacji przy każdorazowym opuszczeniu stanowiska,
 - w przypadku stosowania drukarki przenośnej wymagane jest takie ustawienie drukarki aby nie było możliwości podejrzenia bądź pobrania wydruków przez osoby nieuprawnione.
- Zaleca się wykonywanie kopii bezpieczeństwa zgodnie z opisem w rozdziale 7.2.4.2.
- Zasilanie awaryjne:
 - Stan baterii powinien umożliwiać bezpieczne zamknięcie systemu po zaniku zasilania sieciowego.

8. Wnioskowanie o dostęp do systemu CEPiK 2.0

8.1.Podmioty określone w art. 80ba. ust. 1 ustawy PoRD – zasilanie centralnej ewidencji pojazdów

Podmioty uzyskujące dostęp do systemu CEPiK na podstawie art. 80 bb. ust. 1 ustawy Prawo o ruchu drogowym w związku z art. 80 ba. ust. 1 tej ustawy składają wniosek certyfikacyjny, zgodnie z procedurą określoną w danej polityce certyfikacji, z której podmiot wnioskuje o certyfikat.

W określonych przypadkach może występować konieczność formalnego uregulowania dostępu do systemu CEPiK 2.0 (porozumienie lub umowa) – podmioty będą informowane indywidualnie lub stosowna informacja będzie opublikowana na stronie www.cepik.gov.pl.

8.2.Podmioty określone w art. 80c. ust. 1 ustawy PoRD – dostęp do centralnej ewidencji pojazdów

Podmioty uzyskujące dostęp do systemu CEPiK na podstawie art. 80 c. ust. 1 ustawy Prawo o ruchu drogowym w związku z art. 80 c. ust. 6 tej ustawy składają wniosek o wyrażenie zgody na udostępnienie danych zgromadzonych w ewidencji za pomocą urządzeń teletransmisji danych.

Dopiero po wyrażeniu zgody, w drodze decyzji administracyjnej, podmiot może wystąpić z wnioskiem certyfikacyjnym, zgodnie z procedurą określoną w danej polityce certyfikacji, z której podmiot wnioskuje o certyfikat.

W określonych przypadkach może występować konieczność formalnego uregulowania dostępu do systemu CEPiK 2.0 (porozumienie lub umowa) – podmioty będą informowane indywidualnie lub stosowna informacja będzie opublikowana na stronie www.cepik.gov.pl.

8.3.Podmioty określone w art. 100 ac. ust. 1 ustawy PoRD – zasilanie centralnej ewidencji kierowców

Podmioty uzyskujące dostęp do systemu CEPiK na podstawie art. 100 ad. ust. 1 ustawy Prawo o ruchu drogowym w związku z art. 100 ac. ust. 1 tej ustawy składają wniosek certyfikacyjny, zgodnie z procedurą określoną w danej polityce certyfikacji, z której podmiot wnioskuje o certyfikat.

W określonych przypadkach może występować konieczność formalnego uregulowania dostępu do systemu CEPiK 2.0 (porozumienie lub umowa) – podmioty będą informowane indywidualnie lub stosowna informacja będzie opublikowana na stronie www.cepik.gov.pl.

8.4.Podmioty określone w art. 100 ah. ust. 1 ustawy PoRD – dostęp do centralnej ewidencji kierowców

Podmioty uzyskujące dostęp do systemu CEPiK na podstawie art. 100 ah. ust. 1 ustawy Prawo o ruchu drogowym w związku z art. 100 ah. ust. 5 tej ustawy składają wniosek o wyrażenie zgody na udostępnienie danych zgromadzonych w ewidencji za pomocą urządzeń teletransmisji danych.

Dopiero po wyrażeniu zgody, w drodze decyzji administracyjnej, podmiot może wystąpić z wnioskiem certyfikacyjnym, zgodnie z procedurą określoną w danej polityce certyfikacji, z której podmiot wnioskuje o certyfikat.

W określonych przypadkach może występować konieczność formalnego uregulowania dostępu do systemu CEPiK 2.0 (porozumienie lub umowa) – podmioty będą informowane indywidualnie lub stosowna informacja będzie opublikowana na stronie www.cepik.gov.pl.

8.5.Podmioty określone w art. 100g ust. 2 ustawy PoRD – zasilanie centralnej ewidencji posiadaczy kart parkingowych

Podmioty uzyskujące dostęp do systemu CEPiK na podstawie art. 100 h. ust. 1 ustawy Prawo o ruchu drogowym w związku z art. 100 g. ust. 2 tej ustawy składają wniosek certyfikacyjny, zgodnie z procedurą określoną w danej polityce certyfikacji, z której podmiot wnioskuje o certyfikat.

W określonych przypadkach może występować konieczność formalnego uregulowania dostępu do systemu CEPiK 2.0 (porozumienie lub umowa) – podmioty będą informowane indywidualnie lub stosowna informacja będzie opublikowana na stronie www.cepik.gov.pl.

8.6.Podmioty określone w art. 100 k. ust. 1 ustawy PoRD – dostęp do centralnej ewidencji posiadaczy kart parkingowych

Podmioty uzyskujące dostęp do systemu CEPiK na podstawie art. 100 k. ust. 1 ustawy Prawo o ruchu drogowym w związku z art. 100 k. ust. 3 tej ustawy składają wniosek o wyrażenie zgody na udostępnienie danych zgromadzonych w ewidencji za pomocą urządzeń teletransmisji danych.

Dopiero po wyrażeniu zgody, w drodze decyzji administracyjnej, podmiot może wystąpić z wnioskiem certyfikacyjnym, zgodnie z procedurą określoną w danej polityce certyfikacji, z której podmiot wnioskuje o certyfikat.

W określonych przypadkach może występować konieczność formalnego uregulowania dostępu do systemu CEPiK 2.0 (porozumienie lub umowa) – podmioty będą informowane indywidualnie lub stosowna informacja będzie opublikowana na stronie www.cepik.gov.pl.

8.7.Pozostałe podmioty

Pozostałe podmioty nie wymienione powyżej składają wniosek certyfikacyjny, zgodnie z procedurą określoną w danej polityce certyfikacji, z której podmiot wnioskuje o certyfikat.

W określonych przypadkach może występować konieczność formalnego uregulowania dostępu do systemu CEPiK 2.0 (porozumienie lub umowa) – podmioty będą informowane indywidualnie lub stosowna informacja będzie opublikowana na stronie www.cepik.gov.pl.

8.8.Wnioskowanie

Nowe podmioty, które po raz pierwszy wnioskują o dostęp do systemu CEPiK 2.0, wysyłają wnioski na adres:

**Departament Ewidencji Państwowych
Ministerstwo Cyfryzacji
ul. Królewska 27
00-060 Warszawa**

Podmioty, które posiadają już dostęp do systemu CEPiK 2.0, postępują zgodnie z procedurami określonymi dla odnawiania certyfikatów.

9. Incydenty bezpieczeństwa

Przypadki naruszenia bezpieczeństwa danych osobowych, należy niezwłocznie zgłaszać w formie zawiadomienia pisemnego (niezależnie od własnych polityk i procedur) do Administratora Bezpieczeństwa Informacji w Ministerstwie Cyfryzacji.

Administrator Bezpieczeństwa Informacji

Ministerstwo Cyfryzacji

e-mail: abi@mc.gov.pl

ul. Królewska 27

00-060 Warszawa

adres strony: www.mc.gov.pl

10. Audyty

Podmiotem realizującym na zlecenie Ministerstwa audyty podmiotów wnioskujących o dostęp do CEPiK 2.0 jest:

Centralny Ośrodek Informatyki

ul. Suwak 3

02-676 Warszawa

email: coi@coi.gov.pl

adres strony: www.coi.gov.pl

Audyt obejmuje spełnianie przez Podmiot wymagań określonych powyżej. MC może odstąpić od audytu w toku indywidualnych uzgodnień z danym podmiotem.