Polityka Bezpieczeństwa Systemu Informatycznego Centralnej Ewidencji Pojazdów i Kierowców 2.0

Wymagania, zalecenia i wytyczne bezpieczeństwa dla Użytkowników Indywidualnych korzystających z Aplikacji Dostępowych Systemu Informatycznego Centralnej Ewidencji Pojazdów i Kierowców 2.0

---

wersja 1.00 z dnia 27.09.2017 r.

obowiązują od dnia: 13 listopada 2017 r.

Spis treści

1. Użytkownicy Indywidualni

Użytkownikiem jest każda osoba lub podmiot uprawniony na podstawie przepisów prawa do dostępu do centralnej ewidencji pojazdów (CEP), centralnej ewidencji kierowców (CEK) lub centralnej ewidencji posiadaczy kart parkingowych (CEPKP), posiadająca w Systemie Informatycznym Centralnej Ewidencji Pojazdów i Kierowców 2.0 (SI CEPiK 2.0) jednoznacznie identyfikujące taką osobę lub podmiot konto.

Użytkownik Indywidualny to kategoria Użytkowników SI CEPiK 2.0, którzy korzystają z Aplikacji Dostępowych udostępnianych przez Ministerstwo Cyfryzacji, funkcjonujących w ramach SI CEPiK 2.0.

Aplikacje Dostępowe SI CEPiK 2.0 są to aplikacje funkcjonujące w ramach SI CEPiK 2.0, dostępne przez przeglądarkę internetową, z których Użytkownik może skorzystać, jeżeli nie posiada lub nie chce budować własnego systemu lub aplikacji dziedzinowej zintegrowanych z SI CEPiK 2.0 z wykorzystaniem usług sieciowych (web services).

2. Dokumentacja opisująca sposób przetwarzania danych osobowych

Każdy Użytkownik Indywidualny SI CEPiK 2.0, zgodnie z art. 36 ust 1 *ustawy o ochronie danych osobowych* (UODO) obowiązany jest 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, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem. Zgodnie z art. 36 ust 2 UODO 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 czynności,
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.

3. Środki ochrony kryptograficznej

W SI CEPiK 2.0 stosowane są środki kryptograficznej ochrony danych. Każdy Użytkownik Indywidualny, aby skorzystać z usług SI CEPiK 2.0, musi posiadać odpowiedni certyfikat dostępowy zawierający jego dane i w sposób jednoznaczny go identyfikujący. Ponadto, w przypadku łączenia się z SI CEPiK 2.0 przez sieć publiczną Internet, Użytkownik Indywidualny musi posiadać certyfikat umożliwiający zestawienie bezpiecznego połączenia VPN z SI CEPiK 2.0. Szczegółowy sposób uzyskania certyfikatów, ich wymiany, zasady 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 terminowania sesji 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 Indywidualnych korzystających z Aplikacji Dostępowych funkcjonujących w ramach SI CEPiK 2.0 służące do autoryzacji, uwierzytelniania, podpisywania komunikatów i terminowania sesji SSL (certyfikaty SSL).

ZABRONIONE JEST EKSPORTOWANIE PRZEZ UŻYTKOWNIKÓW INDYWIDUALNYCH KLUCZY PRYWATNYCH Z KART KRYPTOGRAFICZNYCH DO PLIKU, PRZECHOWYWANIE TAKICH PLIKÓW NA STANOWISKU KOMPUTEROWYM, W SZCZEGÓLNOŚCI IMPORTOWANIE DO PRZEGLĄDARKI INTERNETOWEJ LUB SYSTEMU OPERACYJNEGO. KLUCZ PRYWATNY MUSI ZNAJDOWAĆ SIĘ NA KARCIE KRYPTOGRAFICZNEJ.

NA STANOWISKU DOSTĘPOWYM MOŻE BYĆ ZAIMPORTOWANY WYŁĄCZNIE KLUCZ PRYWATNY I ODPOWIADAJĄCY MU CERTYFIKAT DO POŁĄCZEŃ VPN, PRZY CZYM ZAWSZE NALEŻY ZABEZPIECZYĆ HASŁEM O WYSOKIM POZIOMIE TRUDNOŚCI MOŻLIWOŚĆ EKSPORTU TAKIEGO KLUCZA PRYWATNEGO Z SYSTEMU OPERACYJNEGO, OPROGRAMOWANIA VPN LUB URZĄDZENIA SIECIOWEGO.

ZABRONIONE JEST UDOSTĘPNIANIE SWOICH KART KRYPTOGRAFICZNYCH, KODÓW PIN / PUK ORAZ CERTYFIKATÓW VPN INNYM OSOBOM LUB PODMIOTOM.

4. Połączenie z SI CEPiK 2.0

SI CEPiK 2.0 umożliwia Użytkownikom Indywidualnym łączenie się do Aplikacji Dostępowych:

- przez sieć publiczną Internet,
- przez sieć dedykowaną.

Użytkownik Indywidualny łączący się z SI CEPiK 2.0 przez sieć publiczną Internet musi zestawić bezpieczne połączenie VPN z wykorzystaniem certyfikatu VPN. Dopiero po zestawieniu połączenia VPN użytkownik uzyska możliwość wywołania w przeglądarce internetowej Aplikacji Dostępowej SI CEPiK 2.0. Autoryzacja i uwierzytelnienie Użytkownika Indywidualnego w Aplikacjach Dostępowych SI CEPiK 2.0 są realizowane w oparciu o posiadany przez Użytkownika Indywidualnego certyfikat SSL umieszczony na mikroprocesorowej karcie kryptograficznej.

Użytkownik Indywidualny łączący się z systemem CEPiK 2.0 przez sieć dedykowaną ma możliwość wywołania w przeglądarce internetowej Aplikacji Dostępowej CEPiK 2.0 bez konieczności zestawiania bezpiecznego połączenia VPN – autoryzacja i uwierzytelnienie Użytkownika Indywidualnego w Aplikacjach Dostępowych SI CEPiK 2.0 są realizowane w oparciu o posiadany przez Użytkownika Indywidualnego certyfikat SSL umieszczony na mikroprocesorowej karcie kryptograficznej.

System CEPiK 2.0 wspiera rozwiązanie programowe Cisco AnyConnect i komunikację VPN typu Remote Access. Dla tych rozwiązań Service Desk dla SI CEPiK 2.0 zapewni wsparcie związane z instalacją oraz konfiguracją oprogramowania na stanowisku dostępowym.

System CEPiK 2.0 wyłącznie dopuszcza połączenia VPN typu Lan-to-Lan (L2L), przy czym ich nie wspiera. Każdy Użytkownik Indywidualny decydujący się na takie połączenie zestawia je we własnym zakresie, na podstawie podanych parametrów konfiguracyjnych połączenia. Przed implementacją takiego rozwiązania należy skontaktować się z Service Desk dla SI CEPiK 2.0 lub Biurem Programu CEPiK 2.0 w celu poinformowania o chęci skorzystania z połączenia L2L oraz otrzymania niezbędnych danych i informacji, które umożliwią konfigurację urządzeń po stronie Użytkownika. Service Desk dla SI CEPiK 2.0 nie będzie świadczył pomocy w dalszej konfiguracji połączenia po stronie Użytkownika.

5. Wymagania, zalecenia i wytyczne bezpieczeństwa dla Użytkowników Indywidualnych

5.1. Ochrona fizyczna *Pomieszczeń*

W celu zapewnienia odpowiedniego poziomu ochrony *Pomieszczeń*, w których Użytkownicy będą korzystali z Aplikacji Dostępowych SI CEPiK 2.0, w szczególności wymagane jest spełnienie poniżej określonych wymagań.

KORZYSTANIE ZE SPRZĘTU KOMPUERTOWEGO PRZENOŚNEGO I APLIKACJI DOSTĘPOWYCH W CELU DOSTĘPU DO SI CEPiK 2.0 POZA POMIESZCZENIAMI, O KTÓRYCH MOWA W NINIEJSZYM DOKUMENCIE, JEST WYSOCE NIEZALECANE I KAŻDORAZOWO WYMAGA UZYSKANIA ZGODY MINISTERSTWA CYFRYZACJI.

5.1.1. *Pomieszczenia* i ich lokalizacja

5.1.1.1. WYMAGANIA MINIMALNE

- *Pomieszczenia* powinny zapewniać takie rozmieszczenie sprzętu oraz dokumentów, aby uniemożliwić dostęp do informacji osobom nieupoważnionym do dostępu do tej informacji (np. wygrodzenia, żaluzje);
- *Pomieszczenia* powinny być zlokalizowane w miejscach, gdzie ryzyko ich zatopienia lub zalania jest zminimalizowane;

5.1.1.2. WYMAGANIA DODATKOWE

- *Pomieszczenia* nie powinny być pomieszczeniami przechodnimi;
- *Pomieszczenia* powinny być wyposażone w system alarmowy, czujki wilgoci oraz dymu z funkcją powiadomienia służby ochrony lub jednostek straży pożarnej, policji;

5.1.2. Kontrola dostępu do *Pomieszczeń*

5.1.2.1. WYMAGANIA MINIMALNE

- manualna kontrola dostępu do *Pomieszczeń* realizowana jest metodami organizacyjno- proceduralnymi (np. książka pobrań kluczy);
- dostęp do *Pomieszczeń* mogą posiadać wyłącznie osoby uprawnione i upoważnione do przetwarzania danych osobowych. Inne osoby mogą przebywać w *Pomieszczeniach* wyłącznie w obecności osób uprawnionych, za ich wiedzą i zgodą;

5.1.2.2. WYMAGANIA DODATKOWE

- zastosowanie systemu elektronicznej kontroli dostępu do *Pomieszczeń*; urządzenia automatycznej kontroli dostępu winny być nadzorowane całodobowo przez służbę ochrony i okresowo powinna być wykonywana kontrola logów urządzenia;

- dostęp do *Pomieszczeń* mogą mieć tylko osoby uprawnione i upoważnione do przetwarzania danych osobowych; inne osoby mogą przebywać w *Pomieszczeniach* jedynie w obecności osób uprawnionych, za ich wiedzą i zgodą, po odnotowaniu danych osób nieuprawnionych np. w książce wejść osób nieuprawnionych;
- zaleca się zastosowanie systemu elektronicznej kontroli dostępu do *Pomieszczeń* w celu odnotowania wejść osób nieuprawnionych;

5.1.3. Zabezpieczenie drzwi i okien

5.1.3.1. WYMAGANIA MINIMALNE

- drzwi do *Pomieszczeń* znajdujące się wewnątrz budynku w strefie ograniczonego dostępu (bądź dozorowanej), muszą być wyposażone w co najmniej 1 zamek atestowany (zabezpieczenie i odporność na przewiercenie wg PN-EN 12209:2016-04 – klasa 3 lub odporność na włamanie wg KT/402/IMP:2014 – klasa C lub odporność na atak wg PN-EN 1303:2015-07 – klasa 2);
- drzwi do *Pomieszczeń* znajdujące się wewnątrz budynku w strefie ogólnodostępnej niedozorowanej muszą alternatywnie:
  - spełniać wymagania klasy RC 2 zgodnie z normą PN-EN 1627 lub
  - być zabezpieczone przed wyważeniem (podważeniem) oraz być wyposażone w co najmniej 1 zamek atestowany (klasa 3 / klasa C / klasa 2);
- drzwi do *Pomieszczeń*, do których dostęp jest z zewnątrz budynku, muszą:
  - spełniać wymagania co najmniej klasy RC 2 zgodnie z normą PN-EN 1627, oraz
  - posiadać co najmniej jeden zamek atestowany (klasa 3 / klasa C / klasa 2) lub
  - w *Pomieszczeniach* powinien być zainstalowany system alarmowy z funkcją powiadamiania;
- otwory okienne *Pomieszczeń* zlokalizowanych na parterze lub ostatniej kondygnacji (jeśli jest swobodny dostęp do dachu) o ile nie są zabezpieczone kratami:
  - muszą być oklejone folią antywłamaniową lub
  - muszą być w nich zastosowane szyby o wzmocnionej odporności na zbicie;

5.1.3.2. WYMAGANIA DODATKOWE

- drzwi do *Pomieszczeń* znajdujące się wewnątrz budynku w strefie ogólnodostępnej niedozorowanej powinny spełniać wymagania co najmniej klasy RC 2 zgodnie z normą PN-EN 1627 oraz być wyposażone w co najmniej jeden zamek atestowany (klasa 3 / klasa C / klasa 2);
- drzwi do *Pomieszczeń*, do których dostęp jest z zewnątrz budynku powinny spełniać wymagania co najmniej klasy RC 3 zgodnie z normą PN-EN 1627;
- otwory okienne *Pomieszczeń* zlokalizowanych na parterze lub ostatniej kondygnacji (o ile jest swobodny dostęp do dachu) powinny alternatywnie:

- być okratowane lub
- posiadać okna spełniające wymagania co najmniej klasy RC 2 zgodnie z normą PN-EN 1627 z szybą klasy P4A zgodnie z normą PN-EN 356:2000.

5.2. Zabezpieczenia nośników danych

W celu zapewnienia odpowiedniego poziomu ochrony danych przechowywanych na nośnikach danych, w szczególności wymagane jest spełnienie poniżej określonych wymagań.

5.2.1. WYMAGANIA MINIMALNE

- dokumenty i nośniki informacji zawierające dane osobowe należy przechowywać w miejscu uniemożliwiającym dostęp do nich osobom nieupoważnionym (np. w zamykanych na klucz szafkach);
- karty kryptograficzne służące do logowania do Aplikacji Dostępowych SI CEPiK 2.0, należy składować w szafach wyposażonych w co najmniej 1 zamek;
- do likwidacji wydruków dokumentów i nośników informacji należy stosować niszczarki zgodnie z normą DIN66399 o klasie ochrony B i stopniu bezpieczeństwa 3 lub wyższym lub Użytkownik winien posiadać stosowną umowę na niszczenie dokumentów z firmą zewnętrzną;

ZAKAZANE JEST PRZECHOWYWANIE WRAZ Z KARTĄ KRYTOGRAFICZNĄ KODU PIN ORAZ KODU PUK (PIN ADMINISTRACYJNY) DO TEJ KARTY.

ZAKAZANE JEST PRZEKAZYWANIE SWOJEJ KARTY ORAZ KODÓW PIN / PUK INNYM OSOBOM.

5.2.2. WYMAGANIA DODATKOWE

- dane przechowywane na elektronicznych oraz papierowych nośnikach danych powinny być składowane w szafach wyposażonych w co najmniej 1 zamek atestowany (klasa 1 / klasa A / klasa 0);
- karty kryptograficzne służące do logowania, powinny być składowane w metalowych szafach wyposażonych w co najmniej 1 zamek atestowany (klasa 1 / klasa A / klasa 0) lub sejfach;
- do likwidacji wydruków dokumentów i nośników informacji powinno się stosować niszczarki zgodnie z normą DIN66399 o klasie ochrony B i stopniu bezpieczeństwa 4 lub wyższym.

5.3. Zabezpieczenia urządzeń sieciowych

5.3.1. Urządzenia służące do nawiązywania komunikacji za pomocą sieci dedykowanych

5.3.1.1. Zalecenia w zakresie konfiguracji urządzeń

- **Użytkownicy łączący się z SI CEPiK 2.0 przez sieci dedykowane powinni przede wszystkim stosować się do wymagań i zaleceń określonych dla sieci dedykowanej, z której korzystają;**
- urządzenia 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;
    - zaleca się wdrożenie reglamentacji dostępu do sieci np. na podstawie adresów MAC;

5.3.1.2. Zalecenia w zakresie bezpieczeństwa fizycznego urządzeń

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

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

5.3.2.1. Zalecenia w zakresie konfiguracji urządzeń i oprogramowania

- urządzenia sieciowe pozwalające na zestawienie połączeń VPN powinny być zabezpieczone przed nieuprawnionym dostępem osób trzecich:
    - klucze prywatne do certyfikatów VPN zainstalowanych w urządzeniu musza być zabezpieczone w sposób uniemożliwiający dostęp do nich oraz ich wykorzystanie przez osoby nieuprawnione;
    - 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;
    - zaleca się wdrożenie reglamentacji dostępu do sieci np. na podstawie adresów MAC;

- zaleca się wdrożenie polityki blokowania dostępu do i z sieci publicznej Internet w czasie, w którym jest nawiązane połączenie VPN do SI CEPiK 2.0;
- oprogramowanie służące do zestawiania połączeń VPN typu Remote Access np. Cisco AnyConnect powinno być zabezpieczone w taki sposób, aby uniemożliwić dostęp do kluczy prywatnych do certyfikatów VPN osobom nieuprawnionym;

5.3.2.2. Zalecenia w zakresie bezpieczeństwa fizycznego urządzeń

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

5.4. Sprzęt komputerowy stacjonarny

5.4.1. WYMAGANIA MINIMALNE

5.4.1.1. BIOS/UEFI

- wejście i zmiana ustawień BIOS/UEFI wymaga podania hasła;
- wyłączona jest możliwość uruchamiania systemu z sieci lub innych nośników niż dysk twardy komputera;
- długość hasła BIOS/UEFI wynosi nie mniej niż 6 znaków (co najmniej 1 duża litera i 1 cyfra);

5.4.1.2. Konta użytkowników i hasła

- wbudowane konto administratora powinno być używane tylko w przypadku wykonywania czynności administratora;
- każdemu użytkownikowi komputera ma 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 ma wynosić nie mniej niż 10 znaków (hasło złożone co najmniej 1 duża litera, 1 cyfra i znak specjalny), okres ważności hasła nie może być dłuższy niż 30 dni;
- długość hasła konta użytkownika ma wynosić nie mniej niż 8 znaków (hasło złożone co najmniej 1 duża litera, 1 cyfra i znak specjalny), okres ważności hasła nie może być dłuższy niż 30 dni;
- zaleca się wprowadzić procedury sankcjonujące zmianę PIN mikroprocesorowych kart kryptograficznych nie rzadziej niż co 30 dni;
- należy wprowadzić procedury sankcjonujące bezpieczne przechowywanie haseł oraz kart i PIN / PUK, w szczególności zabraniające udostępnia ich innym osobom;

5.4.1.3. Ochrona przed atakami zewnętrznymi (zapora ogniowa)

- zalecane jest zastosowanie zapory ogniowej (rozwiązanie sprzętowe lub programowe) oraz wdrożenie regulacji zapewniających jej bieżącą aktualizację;

5.4.1.4. Sieci Wi-Fi

- do połączenia z sieciami Wi-Fi należy 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);

5.4.1.5. Ochrona antywirusowa

- należy obowiązkowo stosować oprogramowanie antywirusowe oraz:
    - stosować ustawienia zapewniające aktualizację sygnatur antywirusowych na bieżąco lub

    - w przypadku braku dostępu do sygnatur antywirusowych na bieżąco, wdrożyć procedury zapewniające aktualizację sygnatur antywirusowych nie rzadziej niż raz w tygodniu;
- zalecana jest konfiguracja ustawień oprogramowania antywirusowego zapewniająca pełne skanowanie antywirusowe komputera:
    - co najmniej raz w tygodniu w przypadku braku aktualizacji sygnatur na bieżąco lub
    - co najmniej raz w miesiącu, w przypadku aktualizacji sygnatur na bieżąco;
- konfiguracja oprogramowania antywirusowego ma wymuszać skanowanie każdego zewnętrznego nośnika danych (przenośny dysk twardy, pamięć flash) po jego podłączeniu do komputera;

5.4.1.6. Aktualizacja systemu i oprogramowania

- należy stosować systemy operacyjne oraz inne oprogramowanie tylko pochodzące z legalnego źródła, w wersjach posiadających wsparcie producenta co najmniej w zakresie poprawy błędów związanych z bezpieczeństwem;
- zalecana jest konfiguracja ustawień systemu operacyjnego zapewniająca:
    - aktualizację systemu na bieżąco, nie rzadziej niż raz na tydzień, lub
    - w przypadku braku dostępu do repozytorium poprawek online, wdrożenie procedury zapewniającej aktualizację systemu operacyjnego nie rzadziej niż raz w tygodniu;

5.4.1.7. Usuwanie danych

- po kasowaniu danych należy opróżnić „kosz" systemowy;
- zaleca się konfigurację „kosza" systemowego w taki sposób, aby nie przechowywał usuniętych plików;

5.4.1.8. 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;
- należy wdrożyć regulacje zapewniające obsługę pamięci flash oraz dysków przenośnych 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 rozwiązanie sprzętowe lub programowe umożliwiające szyfrowanie danych z użyciem hasła nie krótszego niż 8 znaków (hasło złożone co najmniej 1 duża litera, 1 cyfra i znak specjalny);

5.4.1.9. Rozmieszczenie sprzętu

- wymagane jest takie ustawienie monitora, aby nie było możliwości podejrzenia danych przetwarzanych na ekranie przez osoby nieuprawnione;

- stacja robocza powinna być ustawiona w miejscu uniemożliwiającym do niej dostęp osobom nieuprawnionym;
- wymagane jest ustawienie czasu automatycznego uruchamiania wygaszacza ekranu na maksymalnie 5 minut, wznowienie pracy wymaga podania hasła, obowiązkowe jest blokowanie stacji przez Użytkownika przy każdorazowym opuszczeniu stanowiska;
- wymagane jest takie ustawienie drukarki, aby nie było możliwości podejrzenia bądź pobrania wydruków przez osoby nieuprawnione;

5.4.1.10. Kopie bezpieczeństwa

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

5.4.2. WYMAGANIA DODATKOWE

5.4.2.1. BIOS/UEFI

- uruchomienie komputera wymaga podania hasła;
- długość hasła BIOS wynosi nie mniej niż 8 znaków (co najmniej 1 duża litera i 1 cyfra);

5.4.2.2. Konta użytkowników i hasła

- 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;
- zalecane jest zastąpienie logowania tradycyjnego (login i hasło) logowaniem z użyciem kart mikroprocesorowych, czytników cech biometrycznych, kluczy bezprzewodowych;

5.4.2.3. Ochrona przed atakami zewnętrznymi (zapora ogniowa)

- zaleca się zastosowanie 2 zapór ogniowych – sprzętowej na styku z siecią publiczną Internet oraz programowej na stacji roboczej, oraz wdrożenie regulacji zapewniających ich bieżącą aktualizację;

5.4.2.4. 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);

5.4.2.5. Ochrona antywirusowa

- zaleca się konfigurację oprogramowania zapewniającą pełne skanowanie antywirusowe stanowiska dostępowego co najmniej raz w tygodniu;

5.4.2.6. Aktualizacja systemu i oprogramowania

- zalecane jest włączenie automatycznych aktualizacji systemu oraz oprogramowania, zgodnie z zaleceniami producentów, a w przypadku braku dostępu do repozytorium poprawek online wdrożenie procedury aktualizacji systemu oraz oprogramowania na bieżąco;

5.4.2.7. Usuwanie danych

- zaleca się do usuwania danych, w szczególności tych zapisanych na nośnikach przenośnych, używać dedykowanego do tego celu oprogramowania;

5.4.2.8. Dyski i urządzenia przenośne

- 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;

5.4.2.9. Rozmieszczenie sprzętu

- zalecane jest stosowanie filtrów prywatyzacyjnych zabezpieczających przed możliwością podejrzenia danych przetwarzanych na ekranie przez osoby nieuprawnione;

5.4.2.10. Kopie bezpieczeństwa

- zalecane jest wdrożenie procedury tworzenia kopii zapasowych zapewniające wykonywanie kopii zapasowej nie rzadziej niż raz na 7 dni;
- składowanie kopi zapasowych powinno odbywać się w innym budynku lub pomieszczeniach w odpowiednio zabezpieczonej szafie;

5.4.2.11. Zasilanie awaryjne

- stacje robocze powinny być wyposażone w urządzenia podtrzymujące zasilanie (UPS) lub wpięte do sieci gwarantowanej (z zapewnionym podtrzymaniem napięcia w przypadku utraty zasilania podstawowego) umożliwiające automatyczne bezpieczne zakończenie pracy w przypadku utraty zasilania podstawowego.

5.5. Środowiska wirtualne (maszyny wirtualne)

Maszyny wirtualne mogą być używane do pracy z SI CEPiK 2.0. Ze względu na zwiększone ryzyko związane z utratą danych podczas przenoszenia sprzętu, stosowanie tego rozwiązania **jest NIEZALECANE** i powinno być ograniczone tylko do uzasadnionych przypadków.

5.5.1. WYMAGANIA MINIMALNE

- zabezpieczenia serwerów/stacji udostępniających maszyny wirtualne oraz zabezpieczenia systemu udostępnianego z wykorzystaniem maszyny wirtualnej muszą być co najmniej na poziomie minimalnym opisanym w rozdziale 5.4**Error! Reference source not found.**;
- uprawnienia do katalogu oraz dostęp do folderu udostępnianego należy ograniczyć tylko do użytkowników maszyny wirtualnej;
- uprawnienia do katalogu oraz dostęp do folderu udostępnianego powinny uniemożliwiać skopiowanie pliku maszyny przez osobę inną niż administrator;
- stosowanie maszyn wirtualnych na dyskach przenośnych bądź pamięciach typu flash **jest niezalecane**. W przypadku konieczności stosowania takiego rozwiązania zaleca się, aby:
    - nośnik plików maszyny wirtualnej był w całości zaszyfrowany;
    - wdrożyć regulacje zapewniające prawidłowe posługiwanie się nośnikami oraz prowadzić ewidencję dysków przenośnych lub 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 maksymalnie 5 próbach nieudanego podania hasła do odblokowania nośnika;

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

Sprzęt komputerowy przenośny może być używany do pracy z SI CEPiK 2.0. Ze względu na zwiększone ryzyko związane z utratą danych podczas przenoszenia sprzętu, stosowanie tego rozwiązania **jest NIEZALECANE** i powinno być ograniczone tylko do uzasadnionych przypadków.

W przypadku korzystania z komputerów przenośnych zalecane jest stosowanie zabezpieczeń opisanych w wymaganiach minimalnych oraz wymaganiach dodatkowych.

KORZYSTANIE ZE SPRZĘTU KOMPUERTOWEGO PRZENOŚNEGO I APLIKACJI DOSTĘPOWYCH W CELU DOSTĘPU DO SI CEPiK 2.0 POZA POMIESZCZENIAMI, O KTÓRYCH MOWA W NINIEJSZYM DOKUMENCIE, JEST WYSOCE NIEZALECANE I KAŻDORAZOWO WYMAGA UZYSKANIA ZGODY MINISTERSTWA CYFRYZACJI.

5.6.1. WYMAGANIA MINIMALNE

5.6.1.1. BIOS/UEFI

- wymagane jest stosowanie ustawień wymagań w rozdziale 5.4.1.1, przy czym długość hasła BIOS/UEFI musi być nie krótsza niż 8 znaków;

5.6.1.2. Konta użytkowników i hasła

- wymagane jest stosowanie wymagań opisanych w rozdziale 5.4.1.2;

5.6.1.3. Ochrona przed atakami zewnętrznymi (zapora ogniowa)

- wymagane jest stosowanie wymagań opisanych w rozdziale 5.4.1.3;

5.6.1.4. Sieci Wi-Fi

- wymagane jest stosowanie wymagań opisanych w rozdziale 5.4.1.4;
- **zabronione jest korzystanie z otwartych lub publicznych sieci Wi-Fi, które nie są siecią wewnętrzną Użytkownika;**

5.6.1.5. Ochrona antywirusowa

- wymagane jest stosowanie wymagań opisanych w rozdziale 5.4.1.5;

5.6.1.6. Aktualizacja systemu i oprogramowania

- wymagane jest stosowanie wymagań opisanych w rozdziale 5.4.1.6;

5.6.1.7. Usuwanie danych

- wymagane jest stosowanie wymagań opisanych w rozdziale 5.4.1.7;

5.6.1.8. Dyski i urządzenia przenośne

- wymagane jest stosowanie wymagań opisanych w rozdziale 5.4.1.8;
- dane składowane na dysku stacji przenośnej muszą być umieszczone w obszarze podlegającym szyfrowaniu lub być szyfrowane;

5.6.1.9. Rozmieszczenie sprzętu

- zalecane jest stosowanie wymagań opisanych w 5.4.1.9;

- **wymagane jest ustawienie czasu automatycznego uruchamiania wygaszacza ekranu na maksymalnie 5 minut, wznowienie pracy wymaga podania hasła, obowiązkowe jest blokowanie lub wyłączenie komputera przez Użytkownika przy każdorazowym opuszczeniu stanowiska;**
- należy umieszczać stację przenośną w taki sposób, aby uniemożliwić podgląd ekranu przez osoby nieuprawnione;
- zalecane jest stosowanie filtrów prywatyzacyjnych zabezpieczających przed możliwością podejrzenia danych przetwarzanych na ekranie przez osoby nieuprawnione;
- stacje przenośną w miejscach korzystania powinno się zabezpieczyć linką antykradzieżową przymocowaną do stałego elementu wyposażenia (o ile jest to możliwe);

5.6.1.10. Kopie bezpieczeństwa

- wymagane jest stosowanie ustawień opisanych w rozdziale 5.4.1.10;

5.6.1.11. Zasilanie awaryjne

- stan baterii stacji przenośnej musi umożliwiać bezpieczne zamknięcie systemu po zaniku zasilania sieciowego;

5.6.2. WYMAGANIA DODATKOWE

5.6.2.1. BIOS/UEFI

- zalecane jest stosowanie ustawień opisanych w rozdziale 5.4.2.1, przy czym długość hasła BIOS/UEFI musi być nie krótsza niż 10 znaków;

5.6.2.2. Konta użytkowników i hasła

- zalecane jest stosowanie ustawień opisanych w rozdziale 5.4.2.2;

5.6.2.3. Ochrona przed atakami zewnętrznymi (zapora ogniowa)

- wymagane jest stosowanie ustawień opisanych w rozdziale 5.4.2.3;

5.6.2.4. Sieci Wi-Fi

- wymagane jest stosowanie ustawień opisanych w rozdziale 5.4.2.4, przy czym 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);
- **zabronione jest korzystanie z otwartych lub publicznych sieci Wi-Fi, które nie są siecią wewnętrzną Użytkownika;**

5.6.2.5. Ochrona antywirusowa

- wymagane jest stosowanie ustawień opisanych w rozdziale 5.4.2.5;

5.6.2.6. Aktualizacja systemu i oprogramowania

- wymagane jest stosowanie ustawień opisanych w rozdziale 5.4.2.6;

5.6.2.7. Usuwanie danych

- wymagane jest stosowanie ustawień opisanych w rozdziale 5.4.2.7;

5.6.2.8. Dyski i urządzenia przenośne

- wymagane jest stosowanie ustawień opisanych w rozdziale 5.4.2.8;
- dane składowane na dysku stacji przenośnej muszą być umieszczone w obszarze podlegającym szyfrowaniu lub być szyfrowane;
- zaleca się, aby partycja lub dysk stacji przenośnej, na której są przetwarzane dane był w całości zaszyfrowany przy wykorzystaniu sprzętowego modułu szyfrowania lub programowo, przy użyciu algorytmu AES256;

5.6.2.9. Rozmieszczenie sprzętu

- zalecane jest stosowanie wymagań opisanych w 5.4.2.9;
- należy umieszczać stację przenośną w taki sposób, aby uniemożliwić podgląd ekranu przez osoby nieuprawnione;
- zalecane jest stosowanie filtrów prywatyzacyjnych zabezpieczających przed możliwością podejrzenia danych przetwarzanych na ekranie przez osoby nieuprawnione;
- stacje przenośną w miejscach korzystania powinno się zabezpieczyć linką antykradzieżową przymocowaną do stałego elementu wyposażenia (o ile jest to możliwe);

5.6.2.10. Kopie bezpieczeństwa

- wymagane jest stosowanie ustawień opisanych w rozdziale 5.4.2.10.

6. Incydenty bezpieczeństwa

Przypadki naruszenia bezpieczeństwa SI CEPiK 2.0, w szczególności bezpieczeństwa danych osobowych należy zgłaszać niezwłocznie, w formie zawiadomienia pisemnego (niezależnie od własnych polityk i procedur), do Ministerstwa Cyfryzacji:

Ministerstwo Cyfryzacji
Departament Utrzymania i Rozwoju Systemów
e-mail: sekretariat.duirs@mc.gov.pl
ul. Królewska 27
00-060 Warszawa
adres strony: www.mc.gov.pl

oraz pocztą elektroniczną do administratora systemu CEPiK 2.0 na adres e-mail: adm.cepik@mc.gov.pl

W przypadku naruszenia bezpieczeństwa danych osobowych odpowiedzialność za te dane ponosi Użytkownik systemu, który był zalogowany do systemu w czasie, gdy dane te zostały pobrane z SI CEPiK 2.0. Za dalsze przetwarzanie danych uzyskanych w drodze teletransmisji odpowiedzialność ponosi Użytkownik systemu.

7. Audyty

Ministerstwo Cyfryzacji będąc podmiotem odpowiedzialnym za bezpieczeństwo danych przetwarzanych z wykorzystaniem systemów teleinformatycznych dokłada starań, aby zapewnić jak najwyższy poziom ochrony danych osobowych i ich bezpieczeństwo. Przed umożliwieniem podłączenia produkcyjnego do SI CEPiK 2.0 i wydaniem decyzji administracyjnej formalnie umożliwiającej udostępnienie danych przetwarzanych w zbiorach danych CEP, CEK i CEPKP na podstawie odpowiednio art. 80c ust. 6, art. 100ah ust. 5 oraz 100k ust. 3 *Ustawy z dnia 20 czerwca 1997 roku – Prawo o ruchu drogowym*, Ministerstwo Cyfryzacji może zlecić audyt spełniania wymagań określonych w niniejszym dokumencie przez podmiot wnioskujący o dostęp do SI CEPiK 2.0.

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

Centralny Ośrodek Informatyki
ul. Suwak 3
02-676 Warszawa
email: coi@coi.gov.pl
adres strony: www.coi.gov.pl